**22-11150**

# United States Court of Appeals

*for the*

# Eleventh Circuit

IRA KLEIMAN, as the Personal Representative of the Estate of David Kleiman,

*Plaintiff/Appellant,*

– v. –

CRAIG WRIGHT,

*Defendant/Appellee.*

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF FLORIDA
CASE NO: 9:18-cv-80176-BB
(Hon. Beth Bloom)

# APPELLANT'S APPENDIX – VOLUME TWO

ANDREW BRENNER
BOIES SCHILLER FLEXNER LLP
100 SE 2nd Avenue, Suite 2800
Miami, Florida 33131
abrenner@bsfllp.com

DEVIN (VELVEL) FREEDMAN
ROCHE FREEDMAN LLP
1 SE 3rd Avenue, Suite 1240
Miami, Florida 33131
(305) 753-3675
vel@rochefreedman.com

KYLE W. ROCHE *(Pro Hac Vice)*
ROCHE FREEDMAN LLP
99 Park Avenue, Suite 1910
New York, New York 10016
kyle@rochefreedman.com

*Counsel for Plaintiff/Appellant*

# TABLE OF CONTENTS

**VOLUME I:**



**VOLUME II:**

**VOLUME III:**

**VOLUME VIII:**



**SEALED VOLUME**

**VOLUME IX:**

# TAB 83-1

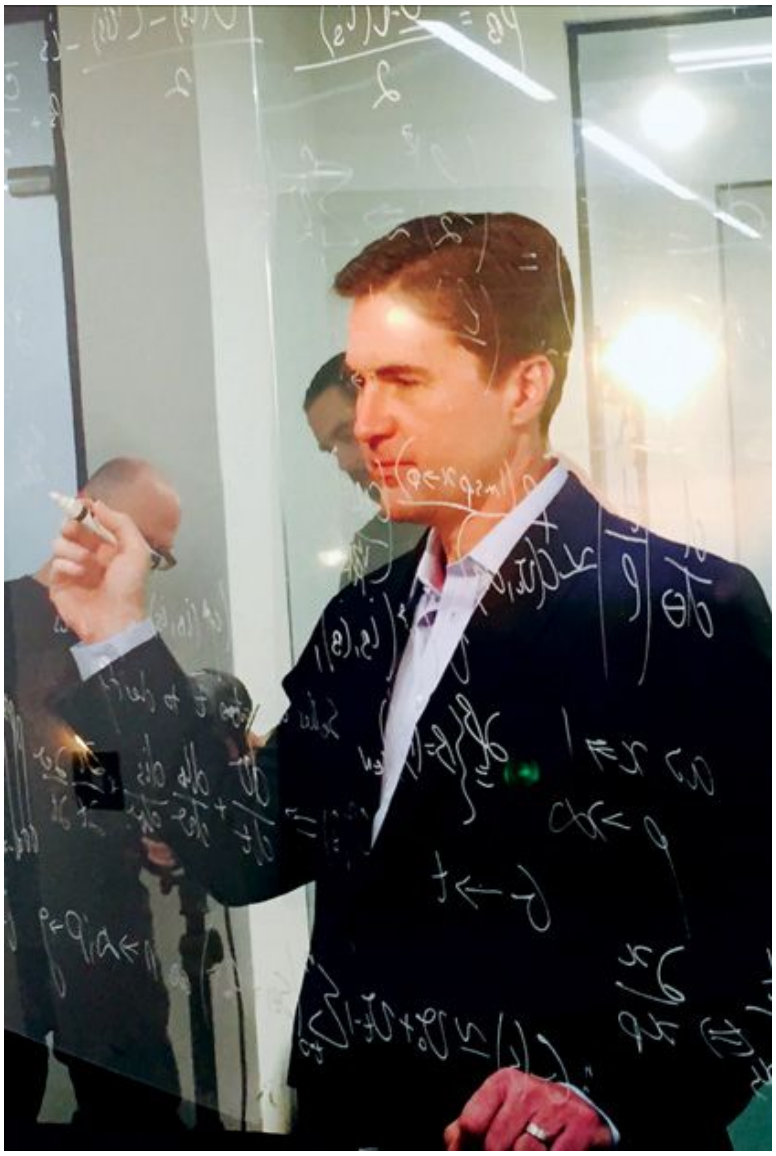
# EXHIBIT 1

# The Satoshi Affair

## Andrew O'Hagan on the many lives of Satoshi Nakamoto

**The Raid**

Ten men raided a house in Gordon, a north shore suburb of Sydney, at 1.30 p.m. on Wednesday, 9 December 2015. Some of the federal agents wore shirts that said 'Computer Forensics'; one carried a search warrant issued under the Australian Crimes Act 1914. They were looking for a man named Craig Steven Wright, who lived with his wife, Ramona, at 43 St Johns Avenue. The warrant was issued at the behest of the Australian Taxation Office. Wright, a computer scientist and businessman, headed a group of companies associated with cryptocurrency and online security. As one set of agents scoured his kitchen cupboards and emptied out his garage, another entered his main company headquarters at 32 Delhi Road in North Ryde. They were looking for 'originals or copies' of material held on hard drives and computers; they wanted bank statements, mobile phone records, research papers and photographs. The warrant listed dozens of companies whose papers were to be scrutinised, and 32 individuals, some with alternative names, or alternative spellings. The name 'Satoshi Nakamoto' appeared sixth from the bottom of the list.



*Craig Wright in the Oxford Circus office.*

Some of the neighbours say the Wrights were a little distant. She was friendly but he was weird – to one neighbour he was 'Cold-Shoulder Craig' – and their landlord wondered why they needed so much extra power: Wright had what appeared to be a whole room full of generators at the back of the property. This fed a rack of computers that he called his 'toys', but the real computer, on which he'd spent a lot of money, was nearly nine thousand miles away in Panama. He had already taken the computers away the day before the raid. A reporter had turned up at the house and Wright, alarmed, had phoned Stefan, the man advising them on what he and Ramona were calling 'the deal'. Stefan immediately moved Wright and his wife into

a luxury apartment at the Meriton World Tower in Sydney. They'd soon be moving to England anyway, and all parties agreed it was best to hide out for now.

At 32 Delhi Road, the palm trees were throwing summer shade onto the concrete walkways – 'Tailor Made Office Solutions', it said on a nearby billboard – and people were drinking coffee in Deli 32 on the ground floor. Wright's office on level five was painted red, and looked down on the Macquarie Park Cemetery, known as a place of calm for the living as much as the dead. No one was sure what to do when the police entered. The staff were gathered in the middle of the room and told by the officers not to go near their computers or use their phones. 'I tried to intervene,' one senior staff member, a Dane called Allan Pedersen, remarked later, 'and said we would have to call our lawyers.'

Ramona wasn't keen to tell her family what was happening. The reporters were sniffing at a strange story – a story too complicated for her to explain – so she just told everyone that damp in the Gordon house had forced them to move out. The place they moved into, a tall apartment building, was right in the city and Wright felt as if he was on holiday. On 9 December, after their first night in the new apartment, Wright woke up to the news that two articles, one on the technology site *Gizmodo*, the other in the tech magazine *Wired*, had come out overnight fingering him as the person behind the pseudonym Satoshi Nakamoto, who in 2008 published a white paper describing a 'peer-to-peer electronic cash system' – a technology Satoshi went on to develop as bitcoin. Reading the articles on his laptop, Wright knew his old life was over.

By this point, cameras and reporters were outside his former home and his office. They had long heard rumours, but the*Gizmodo* and *Wired* stories had sent the Australian media into a frenzy. It wasn't clear why the police and the articles had appeared on the same day. At about five that same afternoon, a receptionist called from the lobby of Wright's apartment building to say that the police had arrived. Ramona turned to Wright and told him to get the hell out. He looked at a desk in front of the window: there were two large laptop computers on it – they weighed a

few kilos each, with 64 gigabytes of RAM – and he grabbed the one that wasn't yet fully encrypted. He also took Ramona's phone, which wasn't encrypted either, and headed for the door. They were on the 63rd floor. It occurred to him that the police might be coming up in the elevator, so he went down to the 61st floor, where there were office suites and a swimming pool. He stood frozen for a minute before he realised he'd rushed out without his passport.

Ramona left the apartment shortly after Wright. She went straight down to the basement car park and was relieved to find the police weren't guarding the exits. She jumped into her car, a hire vehicle, and, in her panic, crashed into the exit barrier. But she didn't stop, and was soon on the motorway heading to north Sydney. She just wanted to be somewhere familiar where she would have time to think. She felt vulnerable without her phone, and decided to drive to a friend's and borrow his. She went to his workplace and took his phone, telling him she couldn't explain because she didn't want to get him involved.

Meanwhile, Wright was still standing beside the swimming pool in his suit, with a laptop in his arms. He heard people coming up the stairs, sped down the corridor and ducked into the gents. A bunch of teenagers were standing around but seemed not to notice him. He went to the furthest cubicle and deliberately kept the door unlocked. (He figured the police would just look for an engaged sign.) He was standing on top of the toilet when he heard the officers come in. They asked the youngsters what they were doing, but they said 'nothing' and the police left. Wright stayed in the cubicle for a few minutes, then went out and used his apartment keycard to hide in the service stairwell. Eventually, a call came from Ramona on her friend's phone. She was slightly horrified to discover he was still in the building and told him again to get out. He, too, had a rental car, and had the key in his pocket. He went down sixty flights of stairs to the car park in the basement, unlocked his car and opened the boot, where he lifted out the spare wheel and put his laptop in the wheel cavity. He drove towards the Harbour Bridge and got lost in the traffic.

*Craig Wright in 2016.*

As Ramona drove along she began texting the mysterious Stefan, who was at Sydney Airport, having already checked in for a flight to Manila, where he lived. Stefan had to make a fuss to get his bag removed from the plane and then he spoke to Ramona, telling her that Wright would have to get out of the country. She didn't argue. She called the Flight Centre and asked what flights were leaving. 'To where?' asked the saleswoman.

'Anywhere,' Ramona said. Within ten minutes she had booked her husband on a flight to Auckland.

In the early evening, Wright, scared and lost, made his way to Chatswood. He texted Ramona to come and meet him, and she immediately texted back saying he should go straight to the airport. She'd booked him a flight. 'But I don't have my passport,' he said. Ramona was afraid she'd be arrested if she returned to their apartment, but her friend said he'd go into the building and get the passport. They waited until the police left the building, then he went upstairs. A few minutes later he came back with the passport, along with the other computer and a power supply.

They met Wright in the airport car park. Ramona had never seen him so worried. 'I was shocked,' he later said. 'I hadn't expected to be outed like that in the media, and then to be chased down by the police. Normally, I'd be prepared. I'd have a bag packed.' As Ramona gave him the one-way ticket to Auckland, she was anxious about when she would see him again. Wright said New Zealand was a bit too close and wondered what to do about money. Ramona went to an ATM and gave him $600. He bought a yellow bag from the airport shop in which to store his computers. He had no clothes. 'It was awful saying goodbye to him,' Ramona said.

In the queue for security, he felt nervous about his computers. His flight was about to close when the security staff flagged him down. He was being taken to an interview room when an Indian man behind him started going berserk. It was just after the Paris bombings; the man's wife was wearing a sari and the security staff wanted to pat her down. The man objected. All the security staff ran over to deal with the situation and told Wright to go. He couldn't believe his luck. He put his head down and scurried through the lounge.

Back at Wright's office, Allan Pedersen was being interviewed by the police. He overheard one of them ask: 'Have we got Wright yet?'

'He's just hopped a flight to New Zealand,' his colleague said.

Wright was soon 30,000 feet above the Tasman Sea watching the programmer Thomas Anderson (Keanu Reeves) being chased by unknowable agents in *The*

*Matrix*. Wright found the storyline strangely comforting; it was good to know he wasn't alone.

At Auckland Airport, Wright kept his phone on flight mode, but turned it on to use the airport's wifi to Skype with Stefan, using a new account. They had a discussion about how to get him to Manila. There was a big rock concert that night in Auckland, and all the hotels were full, but he crossed town in a cab and managed to get a small room at the Hilton. He booked two nights, using cash. He knew how to get more cash out of ATMs than the daily limit, so he worked several machines near the hotel, withdrawing $5000. He ordered room service that night and the next morning went to the Billabong store in Queen Street to buy some clothes. He felt agitated, out of his element: normally he would wear a suit and tie – he enjoys the notion that he is too well dressed to be a geek – but he bought a T-shirt, a pair of jeans and some socks. On the way back to the hotel he got a bunch of SIM cards, so that his calls wouldn't be monitored. Back at the Hilton he was packing up his computers when the dependable Stefan came on Skype. He told Wright to go to the airport and pick up a ticket he'd left him for a flight to Manila. His picture was all over the papers, along with the story that he was trying to escape.

Within hours of Wright's name appearing in the press, anonymous messages threatened to reveal his 'actual history'. Some said he had been on Ashley Madison, the website that sets up extramarital affairs, others that he'd been seen on Grindr, the gay hook-up app. During a six-hour layover in Hong Kong, he killed his email accounts and tried to wipe his social media profile, which he knew would be heavy with information he wasn't keen to publicise: 'Mainly rants,' he said later. When he got to Manila airport, Stefan picked him up. They went to Stefan's apartment and the maid washed Wright's clothes while he set up his laptops on the dining-room table. They spent the rest of Saturday wiping his remaining social media profile. Stefan didn't want any contact to be possible: he wanted to cut Wright off from the world. The next day he put him on a plane to London.

**Mayfair**

Technology is constantly changing the lives of people who don't really understand it – we drive our cars, and care nothing for internal combustion – but now and then a story will break from that frontier. I was one of the people who had never heard of Satoshi Nakamoto or the blockchain – the invention underlying bitcoin, which verifies transactions without the need for any central authority – or that it is the biggest thing in computer science. It was news to me that the banks were grabbing onto the blockchain as the foundation of a future 'internet of value'. The story of a mythical computer scientist was an odd one to come my way. I'm not much detained by thoughts of new computer paradigms. (I'm still getting the hang of the first one.) But to those who are much more invested in the world of tomorrow, the Satoshi story has the lineaments of a modern morality tale quite independent of stock realities. There are things, there are always things, that others assume are at the centre of the universe but don't make a scratch on your own sense of the everyday world. This story was like that for me, enclosing me in an enigma I couldn't have named. A documentary is a fashioned thing, of course, as fashioned as fiction in its own ways, but I had to overcome my own bafflement – as will you – to enter this world.

A few weeks before the raid on Craig Wright's house, when his name still hadn't ever been publicly associated with Satoshi Nakamoto, I got an email from a Los Angeles lawyer called Jimmy Nguyen, from the firm Davis Wright Tremaine (self-described as 'a one-stop shop for companies in entertainment, technology, advertising, sports and other industries'). Nguyen told me that they were looking to contract me to write the life of Satoshi Nakamoto. 'My client has acquired life story rights … from the true person behind the pseudonym Satoshi Nakamoto – the creator of the bitcoin protocol,' the lawyer wrote. 'The story will be [of] great interest to the public and we expect the book project will generate significant publicity and media coverage once Satoshi's true identity is revealed.'

Journalists, it turned out, had spent years looking for Nakamoto. His identity was one of the great mysteries of the internet, and a holy grail of investigative reporting, with writers who couldn't dig up evidence simply growing their own. For the*New*

*Yorker*'s Joshua Davis the need to find him seemed almost painful. 'Nakamoto himself was a cipher,' he wrote in October 2011:

> Before the debut of bitcoin, there was no record of any coder with that name. He used an email address and a website that were untraceable. In 2009 and 2010, he wrote hundreds of posts in flawless English, and though he invited other software developers to help him improve the code, and corresponded with them, he never revealed a personal detail. Then, in April 2011, he sent a note to a developer saying that he had 'moved on to other things'. He has not been heard from since.

Davis went on to examine Satoshi's writing quite closely and concluded that he used British spelling and was fond of the word 'bloody'. He then named a 23-year-old Trinity College Dublin graduate student, Michael Clear, who quickly denied it. The story went nowhere and Clear went back to his studies. Then Leah McGrath Goodman wrote a piece for *Newsweek*claiming Satoshi was a maths genius called Dorian Nakamoto, who lived in the Californian suburb of Temple City and didn't actually know, it turned out, how to pronounce bitcoin. When Goodman's article ran on the magazine's cover reporters from all over the world arrived on Dorian's doorstep. He said he would give an interview to the first person who would take him to lunch. It turned out that his hobby wasn't alternative currencies but model trains. Someone calling himself Satoshi Nakamoto, and using Satoshi's original email address, visited one of the forums Satoshi used to haunt and posted the message: 'I am not Dorian Nakamoto.' Other commentators, including Nathaniel Popper of the *New York Times*, named Nick Szabo, a cool cryptocurrency nut and the inventor of Bit Gold, but he denied it profusely. *Forbes* believed it was Hal Finney, who, the blockchain irrefutably showed, was the first person in the world to be sent bitcoin by Satoshi. Finney, a native Californian, was an expert cryptographer whose involvement in the development of bitcoin was vital. He was diagnosed with motor neurone disease in 2009 and died in 2014. It came to seem that the holy grail would remain out of reach. 'Many in the bitcoin community … in deference to the bitcoin creator's clear desire for privacy … didn't want to see the wizard unmasked,' Popper wrote in the *New York Times*. 'But even among those who said this, few could resist debating the clues the founder left behind.'

The 'Stefan' who was hovering during the raid on Craig Wright's house and office is Stefan Matthews, an IT expert whom Wright had known for ten years, since they both worked for the online gambling site Centrebet. In those days, around 2007, Wright was often hired as a security analyst by such firms, deploying his skills as a

computer scientist (and his experience as a hacker) to make life difficult for fraudsters. Wright was an eccentric guy, Stefan Matthews remembered, but known to be a reliable freelancer. Matthews said that Wright had given him a document to look at in 2008 written by someone called Satoshi Nakamoto, but Matthews had been busy at the time and didn't read it for a while. He said that Wright was always trying to get him interested in this new venture called bitcoin. He tried to sell him 50,000 coin for next to nothing, but Matthews wasn't interested, he told me, because Wright was weird and the whole thing seemed a bit cranky. A few years later, however, Matthews realised that the document he had been shown was, in fact, an original draft of the by now famous white paper by Satoshi Nakamoto. (Like the governments they despise, bitcoiners deal – when it comes to ideas – in 'white papers', as if they were issuing laws.) Last year, when Wright was in financial trouble, he approached Matthews several times. By that time, Matthews had become friendly with Robert MacGregor, the founder and CEO of a Canada-based money-transfer firm called nTrust. Matthews encouraged MacGregor to come to Australia and assess Wright's value as an investment opportunity. Wright had founded a number of businesses that were in trouble and he was deeply embedded in a dispute with the ATO. Nevertheless, Matthews told MacGregor, Wright was almost certainly the man behind bitcoin.

Matthews argued that since Satoshi's disappearance in 2011, Wright had been working on new applications of the blockchain technology he had invented as Satoshi. He was, in other words, using the technology underlying bitcoin to create new versions of the formula that could, at a stroke, replace the systems of bookkeeping and registration and centralised authority that banks and governments depend on. Wright and his people were preparing dozens of patents, and each invention, in a specific way, looked to rework financial, social, legal or medical services, expanding on the basic idea of the 'distributed public ledger' that constitutes the blockchain. This is utopian thinking, even by normal geek standards,

but it's a hot topic in computer science and banking at the moment, and hundreds of millions of dollars are being invested in such ideas. Thus: Matthews's proposal.

After initial scepticism, and in spite of a slight aversion to Wright's manner, MacGregor was persuaded, and struck a deal with Wright, signed on 29 June 2015. MacGregor says he felt sure that Wright was bitcoin's legendary missing father, and he told me it was his idea, later in the drafting of the deal, to insist that Satoshi's 'life rights' be included as part of the agreement. Wright's companies were so deep in debt that the deal appeared to him like a rescue plan, so he agreed to everything, without, it seems, really examining what he would have to do. Within a few months, according to evidence later given to me by Matthews and MacGregor, the deal would cost MacGregor's company $15 million. 'That's right,' Matthews said in February this year. 'When we signed the deal, $1.5 million was given to Wright's lawyers. But my main job was to set up an engagement with the new lawyers … and transfer Wright's intellectual property to nCrypt' – a newly formed subsidiary of nTrust. 'The deal had the following components: clear the outstanding debts that were preventing Wright's business from getting back on its feet, and work with the new lawyers on getting the agreements in place for the transfer of any non-corporate intellectual property, and work with the lawyers to get Craig's story rights.' From that point on, the 'Satoshi revelation' would be part of the deal. 'It was the cornerstone of the commercialisation plan,' Matthews said, 'with about ten million sunk into the Australian debts and setting up in London.'

The plan was always clear to the men behind nCrypt. They would bring Wright to London and set up a research and development centre for him, with around thirty staff working under him. They would complete the work on his inventions and patent applications – he appeared to have hundreds of them – and the whole lot would be sold as the work of Satoshi Nakamoto, who would be unmasked as part of the project. Once packaged, Matthews and MacGregor planned to sell the intellectual property for upwards of a billion dollars. MacGregor later told me he was speaking

to Google and Uber, as well as to a number of Swiss banks. ‘The plan was to package it all up and sell it,’ Matthews told me. ‘The plan was never to operate it.’

*Clockwise from top left: Hal Finney, Gavin Andresen, Robert MacGregor, Stefan Matthews*

*

Since the time I worked with Julian Assange, my computers have been hacked several times. It isn’t unusual for me to find that material has been wiped, and I was careful to make sure the lawyer’s approach wasn’t part of a sting operation. But I was curious to see what these men had. I assumed MacGregor – or someone behind him – must be the ‘client’ referred to in the email I had received from California. On Thursday, 12 November, I turned up at MacGregor’s office near Oxford Circus, where I signed in under a pseudonym and made my way to a boardroom wallpapered with mathematical formulae. MacGregor came into the room wearing a tailored jacket and jeans, with a blue-edged pocket square in his breast pocket, a scarf and brown brogue boots. He was 47 but looked about 29. There was something studied about him – the Alexander McQueen scarf, the lawyerly punctilio – and I’d never met anyone who spoke so easily about such large

sums of money. When I asked him the point of the whole exercise he said it was simple: ‘Buy in, sell out, make some zeroes.’

MacGregor described Wright to me as ‘the goose that lays the golden egg’. He said that if I agreed to take part I would have exclusive access to the whole story, and to everyone around Wright, and that it would all end with Wright proving he was Satoshi by using cryptographic keys that only Satoshi had access to, those associated with the very first blocks in the blockchain. MacGregor told me this might happen at a public TED talk. He said it would be ‘game over’. Wright’s patents would then be sold and Wright could get on with his life, out of the public eye. ‘All he wants is peace to get on with his work,’ MacGregor told me at that first meeting. ‘And how this ends, for me, is with Craig working for, say, Google, with a research staff of four hundred.’

I told MacGregor that there would have to be a process of verification. We talked about money, and negotiated a little, but after several meetings I decided I wouldn’t accept any. I would write the story as I had every other story under my name, by observing and interviewing, taking notes and making recordings, and sifting the evidence. ‘It should be warts and all,’ MacGregor said. He said it several times, but I was never sure he understood what it meant. This was a changing story, and I was the only one keeping account of the changes. MacGregor and his co-workers were already convinced Wright was Satoshi, and they behaved, to my mind, as if that claim was the end of the story, rather than the beginning.

I don’t mean to imply anything sinister. The company was excited by the project and so was I. Very quickly we were working hand in hand: I reserved judgment (and independence) but I was very caught up in the thought of the story unfolding as planned. At this point, nobody knew who Craig Wright was, but he appeared, from the initial evidence, to have a better claim to being Satoshi Nakamoto than anyone else had. He seemed to have the technical ability. He also had the right social history, and the timeline worked. The big proof was up ahead, and how could it not be spectacular? I went slowly forward with the project, and said no to everything

that would hamper my independence. This would become an issue later on with MacGregor and Matthews, or the men in black, as I'd taken to calling them, but for those first few months, nobody asked me to sign anything and nobody refused me access. Mysteries would open up, and some would remain, but there seemed no mystery about the fact that these people were confident that a supremely important thing was happening and that the entire process should be witnessed and recorded. My emails to MacGregor took it for granted that what would be good for my story, in terms of securing proof, would also be good for his deal, and that seemed perfectly true. Yet I feel bad that I didn't warn him of the possibility that this might not be what happened, that my story wouldn't die if the deal died, that human interest doesn't stop at success.

It was at this point, four weeks after my first meeting with MacGregor, that *Wired* and *Gizmodo* reported that he might be Satoshi. The news unleashed a tsunami of responses from the cryptocurrency community, and most of it was bad for Wright's credibility. Had he left artificial footprints to suggest his involvement with bitcoin had been earlier than it was? Had he exaggerated the number and nature of the degrees he'd accumulated from various universities? Why did the company that supplied the supercomputer he claimed to have bought with amassed bitcoin say it had never heard of him?

'The smell,' as one commentator said, 'was a mile high.' The nCrypt people were unfazed by this mudslinging, believing that every one of the charges made against Wright could be easily disproved. Wright produced an impressive paper showing that his 'footprint' wasn't faked and that the 'cryptographic' evidence against him was bogus (people continue to argue on this point). He produced a letter from the supercomputer supplier acknowledging the order. Charles Sturt University provided a photocopy of his staff card, proving he had lectured there, and Wright sent me a copy of the thesis he'd submitted for a doctorate his critics claim he doesn't have.

*

I had arrived five minutes early at 28-50 Degrees, a wine bar and restaurant in Mayfair. It was just before 1 p.m. on 16 December and the lunchtime crowd, men in blue suits and white shirts, were eating oysters and baby back ribs and drinking high-end wine by the glass. A jeroboam of Graham's ten-year-old tawny port stood on the bar, and I was inspecting it when MacGregor arrived with Mr and Mrs Smith. That's what he'd been calling them in his emails to me. Craig Wright, 45 years old, wearing a white shirt under a black jacket, a pair of blue chinos, a belt with a large Armani buckle and very green socks, wasn't the kind of guy who seems comfortable in a swish restaurant. He sat across from me and lowered his head and at first he let MacGregor do the talking. Ramona was very friendly, chatting about their time in London as if they were a couple of holidaymakers who'd just blown into Mayfair. She wasn't drinking, but the rest of us ordered a glass of Malbec each. When Wright lifted his head to laugh at something, I noticed he had a nice smile but uneven teeth, and a scar that climbed from the top of his nose to the area just above his left eyebrow. He hadn't shaved since he'd left Sydney.

Wright told me he was rubbish at small talk. He too wanted what I wrote to be 'warts and all'; he felt he was being misunderstood by everybody, and normally that wouldn't bother him but he had to consider the respectability of his work, and his family's rights. He appeared to ponder this for a moment, then he told me his old neighbours at the house in Gordon hadn't been friendly.

'They barely even knew your name,' Ramona said.

'They do now,' he replied.

I found him easier to talk to than I'd expected. He said his father had worked for the NSA (he couldn't explain this), but that, to this day, his mother thinks he worked for Nasa. 'The few people I care about I care about a lot,' he said, 'and I care about the state of the world. But there's not much in between.' He said he was happy I was writing about him because he wanted 'to step into history', but mainly because he wanted to tell the story of the brilliant people he had collaborated with. He and

Ramona were both jet-lagged and anxious about things back home. ‘We should have been having our company’s Christmas party today,’ Ramona said.

MacGregor asked Wright if being a libertarian had influenced his work, or if the work had turned him into a libertarian. ‘I was always libertarian,’ he replied, and then he told me his father had more or less kidnapped him after his parents got divorced. He hated being told what to do – that was one of his main motivations. He believed in freedom, and in what freedom would come to mean, and he said his work would guarantee a future in which privacy was protected. ‘Where we are,’ he said, ‘is a place where people can be private and part of that privacy is to be someone other than who they were. Computing will allow you to start again, if you want to. And that is freedom.’ In fact he never stopped imagining different lives for himself. That afternoon he seemed preoccupied by the case people were making against his being Satoshi. He shook his head a lot and said he wished he could just get on in silence with his work. ‘If you want to stay sane through this, ignore Reddit,’ his wife told him.

The next day, 17 December, we met again, in a private room in Claridge’s. You could see outside, over the rooftops, cranes garlanded in fairy lights. Ramona came in looking tired and totally fed up. From time to time, especially when exhausted, she would resent the hold these people had over them. ‘We have sold our souls,’ she said to me in a quiet moment.

MacGregor said he would spend the evening preparing paperwork to be signed by Wright the following day. This would effectively be the final signing over to nCrypt of the intellectual property held by Wright’s companies. This was the main plank in the deal. MacGregor was confident the work was ‘world historical’, that it would change the way we lived. He regularly described the blockchain as the greatest invention since the internet. He said that what the internet had done for communication, the blockchain would do for value.

MacGregor explained that Wright's Australian companies were being signed over to nCrypt and that he'd extended an 'olive branch' to the ATO, which had responded quickly and positively. A lot of trouble with the ATO had to do with whether bitcoin was a commodity or a currency and how it should be taxed. It also had doubts about whether Wright's companies had done as much research and development as they claimed, and whether they were therefore entitled to the tax rebates they had applied for. The ATO had said it couldn't see where the spending was going. Some critics in the media claimed Wright's companies had been set up only for the purpose of claiming rebates, though not even the ATO went that far.

Wright told me that thanks to the tax office they'd had to lay out all the research for their patents, which had been useful since the nCrypt team was in a hurry: the banks, now alert to cryptocurrencies and the effectiveness of the blockchain, are rushing to create their own versions. At that moment, Bank of America was patenting ten ideas for which Craig and his team told me they had a claim to 'prior art'. Governments spent a long time denying the value of bitcoin – seeing it as unstable, or the currency of criminals – but now they celebrate the potential of the technology behind it.

'They're behaving like children,' Wright said of the ATO.

MacGregor looked at his watch. He straightened his cuffs. 'I see this as a pivotal moment in history … It's like being able to go back in time and watch Bill Gates in the garage.' He turned to Wright. 'You released this thing into the wild. Some people got it right and some people got it wrong. But you've got a vision of where it's going next and next and next.'

'None of this would have worked without bitcoin,' Wright said, 'but it's a wheel and I want to build a car.'

Ramona looked depressed. She was worried that her husband, as the person claiming to have invented bitcoin, might be held liable for the actions of those who'd

used the currency for nefarious purposes. ‘He didn’t issue a currency,’ MacGregor assured her. ‘This is just technology – it is not money.’ Ramona was still anxious. ‘We’re talking about legal risk … I’m giving you the legal answer,’ MacGregor said. ‘I would stake my career on the fact that the creation of bitcoin is not a prosecutable event.’

Right to the end, the Wrights would express worries about things Craig did as a young computer forensics worker. Much of his professional past looked questionable, but in the meeting room at Claridge’s he simply batted the past away. ‘It’s what you’re doing now that matters. I’m not perfect. I never will be … All these different people arguing about what Satoshi should be at the moment, it’s crazy.’

**Ninjutsu**

Wright’s father, Frederick Page Wright, was a forward scout in Vietnam, serving with the 8th Battalion of the Australian army. ‘He lost all his friends,’ Wright told me, ‘every single one of them’ – and before long he was drinking and being violent towards Wright’s mother, who eventually left him. Both Wright and his mother, when I went to meet her in Brisbane in March, told me about his father’s anger at his own mother: he sent all his army pay cheques home to her and she spent them while he was away. He also dreamed of a football career that never happened. ‘I have a chip on my shoulder,’ Wright said, ‘but his was bigger.’

‘Did you admire him?’

‘He never admired me. I was never fucking good enough. We played chess from when I was three or four and if I made a wrong move he’d wallop me. We clashed right from the beginning.’

The boy had two great influences. The first was his grandfather Ronald Lyman, who his family claims received the first degree awarded by the Marconi School of Wireless in Australia, and who served in the army as a signals officer. They also say he later became a spy with the Australian security services. Craig’s favourite place

was his grandfather's basement, a paradise of early computing. 'We'd sit there and look at these books of log tables,' he told me. 'I loved doing it.' Captain Lyman had an old terminal and a Hayes 80-103A modem that they used to connect to the University of Melbourne's network. To keep Craig quiet while he worked, Pop, as the children called him, would let him write code. 'I found this community of hackers,' Wright says, 'and I worked out how to interact with them. I started building games and hacking other people's games. In time, I'd be pulling apart hacker code, and eventually I did this for companies, to help them create defences against hackers.'

His mother told me he was sometimes picked on at school. 'He struggled,' she said, 'but after a while I sent him to Padua College' – a private Catholic college in Brisbane – 'and he shone there. I mean, he was different. He used to dress up and he had an obsession with Japanese culture. He had big samurai swords.'

'As a teenager?'

'Dressed up in samurai clothes, with the odd wooden shoes and everything. Making all the noises. His sisters would complain about him embarrassing them: "We're down the park, we've got friends down there, and he's walking around with webbed feet." He used to have this group of nerdy friends in the 1980s: they'd come around in horn-rimmed glasses and play Dungeons & Dragons for hours.'

He had a karate teacher called Mas who moved him quickly from karate through judo to Ninjutsu. Craig broke his knuckles over and over again and 'became stronger', he told me, because 'the pain led to a "me" that could handle more.' The thing that attracted him most to martial arts was the discipline. Learning to become a ninja involves 18 disciplines, including *bōjutsu*(tactics), *hensōjutsu* (disguise and impersonation), *intonjutsu*(escape and concealment) and *shinobi-iri* (stealth and infiltration). He walked home from his lessons feeling stronger, like another self.

When he was 18, Wright joined the air force. ‘They locked me in a bunker,’ he told me, ‘and I worked on a bombing system. Smart bombs. We needed fast code, and I did that.’ When he was in his twenties a melanoma appeared on his back and he had several skin grafts. ‘This was after he got out of the air force,’ his mother told me, ‘and when he recovered he was off to university, and it’s been degrees, degrees, degrees since then.’ He went to the University of Queensland to study computer systems engineering. And over the following 25 years he would finish, or not finish, or finish and not do the graduation paperwork for degrees in digital forensics, nuclear physics, theology, management, network security, international commercial law and statistics. After our first full interview, he went home to work on an assignment for a new course he was taking at the University of London, a masters in quantitative finance.

Over the months I spent with him, I noticed that he loved the idea of heroism and was strongly attracted to creation myths. One of the first things he emailed me was a copy of one of his dissertations, ‘Gnarled Roots of a Creation Mythos’. I noticed it was dedicated to Mas, his martial arts instructor. The text wasn’t merely an argument for self-invention, but a feminist exegesis that railed against patriarchal views of the Fall. Wright also speaks of the pilgrim-visitor in the ‘world garden’. ‘While in the garden, the pilgrim almost inevitably suffers deception. His or her senses, enchanted by illusory and transitory formal appearances, betray his or her soul and lead to sin.’

Wright said he had never expected the myth of Satoshi to gather such force. ‘We were all used to using pseudonyms,’ he told me. ‘That’s the cypherpunk way. Now people want Satoshi to come down from the mountain like a messiah. I am not *that*. And we didn’t mean to set up a myth that way.’ Satoshi was loved by bitcoin fans for making a beautiful thing and then disappearing. They don’t want Satoshi to be wrong or contradictory, boastful or short-tempered, and they don’t really want him to be a 45-year-old Australian called Craig.

While reading Wright's ideas on creation, I kept thinking of his karate teacher and the position he had in the young man's life. An offhand remark Wright made had stayed with me. It was about storytelling and how a possible meaning of freedom might reside not only in martial arts, in the ability to defend oneself, but in the ability to make oneself. Mas 'taught me a lot of Eastern philosophy and gave me the means to become myself', Wright said. One day Mas told him about Tominaga Nakamoto. 'He was a Japanese merchant philosopher,' Wright told me. 'I read translations of his stuff, material from the 1740s.'

Weeks later, I was in the kitchen of the house Wright was renting in London drinking tea with him when I noticed a book on the worktop called *Visions of Virtue in Tokugawa Japan.*I'd done some mugging up by then and was keen to nail the name thing.

'So that's where you say you got the Nakamoto part?' I asked. 'From the 18th-century iconoclast who criticised all the beliefs of his time?'

'Yes.'

'What about Satoshi?'

'It means "ash",' he said. 'The philosophy of Nakamoto is the neutral central path in trade. Our current system needs to be burned down and remade. That is what cryptocurrency does – it is the phoenix …'

'So *satoshi* is the ash from which the phoenix …'

'Yes. And Ash is also the name of a silly Pokémon character. The guy with Pikachu.' Wright smiled. 'In Japan the name of Ash is Satoshi,' he said.

'So, basically, you named the father of bitcoin after Pikachu's chum?'

‘Yes,’ he said. ‘That’ll annoy the buggery out of a few people.’ This was something he often said, as if annoying people was an art.

Wright’s generation, now in their mid to late forties, are seeing a world that enlarges on their teenage kicks. For Wright, as for Jeff Bezos, the rules of how to shop and how to think and how to live are extrapolations of dreams they had sitting in a box room somewhere. ‘The person who experiences greatness must have a feeling for the myth he is in,’ Frank Herbert wrote in*Dune*, Wright’s favourite novel as a teenager. ‘*Dune* was really about people,’ Wright told me. ‘It was about the idea that we don’t want to leave things to machines and [should instead] develop as humans. But I see things a little differently from Mr Herbert. I see that it’s not one or the other – man or machines – it’s a symbiosis and a way of becoming something different together.’ This kind of cyberpunk energy – as opposed to cypherpunk, which came later – delivered Wright’s generation of would-be computer scientists into the brightness of the future.

After getting his first degree, Wright settled into IT roles in a number of companies. He became a well-known ‘go-to guy’ among startups and security firms: he always solved the problem and they always came back for more. ‘When I’ve characterised Craig to colleagues and friends,’ Rob Jenkins, who worked with Wright in this period and now holds a senior position in Australia’s Westpac Bank, told me, ‘I’ve always described him as the most qualified person I’ve ever known. I’ve worked with other smart people but Craig has such a strong desire to pursue knowledge. He has passion. And bitcoin was just another one of those bright things he was talking about.’

‘Sketch it out for me,’ I said to Wright. ‘Those years before bitcoin. What was happening that would later have an influence? I want to know about all the precursors, all the previous attempts to solve the problem.’

‘Back in 1997 there was Tim May’s BlackNet …’ May was a crypto-anarchist, who had been operating and agitating in the cypherpunk community since the mid-1980s. ‘Computer technology is on the verge of providing the ability for individuals and groups to communicate and interact with each other in a totally anonymous manner,’ he wrote in the *Crypto-Anarchist Manifesto in 1988*. BlackNet

operated like a precursor to WikiLeaks, soliciting secret information with payments made by untraceable, digital money.

‘We all have a narcissistic hubris,’ Wright told me. He wanted to take May’s BlackNet idea further. He was also enthusiastic, in those early days, about Hashcash and B-money. The idea behind Hashcash, a ‘proof of work’ algorithm where each of a group of computers performs a small task that can be instantly verified (thus making life impossible for spammers, who depend on multiple emails going out with little to no work involved), was ‘totally necessary for the building of bitcoin’. Wright said that he spoke to Adam Back, who proposed Hashcash in 1997, ‘a few times in 2008, whilst setting up the first trials of the bitcoin protocol’.

B-Money was invented by a man called Wei Dai. At the time of its creation, Wei wrote a paper which assumed ‘the existence of an untraceable network, where senders and receivers are identified only by digital pseudonyms (public keys) and every message is signed by its sender and encrypted to its receiver.’ The public key, or address, is matched, as John Lanchester handily described it in the *LRB*, to ‘a private key which provides access to that address’. A key is really just a string of numbers and digits: the public key demonstrates ownership of any given address; the private key can only be used by the owner of that address. Wei went on to suggest a system for the exchange and transfer of money. ‘Anyone can create money by broadcasting the solution to a previously unsolved computational problem,’ he wrote. The system had methods for rewarding work and keeping users honest. ‘I admired B-Money,’ Wright told me, ‘and he definitely gave me some of the cryptographic code that ended up in the first version of bitcoin.’ Wright was always careful to give credit to those early developers. ‘Wei was very helpful,’ he went on, but ‘to people like that bitcoin seems a bit of a fudge. It works, but it’s not mathematically elegant.’

‘Wei said that?’

‘Wei was very polite. But others said it: Adam Back, Nick Szabo. They would probably like to find a more elegant solution to the problem. Perhaps they see the mining system in bitcoin as wasteful: there’s wasted computation in my system –

machines which are trying to solve problems and not winning. But that's like society.'

'Are these early cryptocurrency people in a state of rivalry?'

'Yes, but it doesn't matter.'

**Kleiman**

The flat in Marylebone where I interviewed Wright had wooden shutters and modern ornaments and pictures, mainly of crows. I set the flat up for work while Craig and Ramona were in the City signing over his intellectual property, and all his companies, to MacGregor. They arrived at the flat a couple of hours late. 'When did you realise the whole Satoshi thing wasn't going to be a secret for ever?' I asked.

'Very recently,' Wright said. 'I didn't really believe it would need to come out. What we believed is that we could leave it in doubt – we wouldn't have to sign using the Satoshi keys or anything else. We have hundreds of patents and papers in progress – research from the beginning – and in the next year we're going to start releasing them. We thought people could suspect and people could query and we could leave it like that.'

'And how did that change?'

Ramona said a single word: 'Rob.'

The days in St Christopher Place were almost languorous. We would bring coffee back to the flat and spread out, and I'd try to build a picture of how he did what he said he did. We put up whiteboards and he bamboozled me with maths. Sometimes he would write at the board for hours, then tear open books and point to theories and proofs. I talked to the scientists he worked with, many of whom were better explainers than he was. One of the things I noticed was that Wright hated claiming outright to be Satoshi and would spend hours giving credit to everyone who had

ever contributed. It was odd: we were in the room because he was coming out as Satoshi, yet the claim embarrassed him and I have many hours of tape in which he deflects it. I felt this unwillingness supported his claim because it showed a proper regard for the communal nature of the work. He was contradictory enough sometimes to enjoy the limelight and actively court it, and this would cause trouble for him, but the idea of speaking directly as Satoshi seemed to fill him with dread. 'I'm afraid that they're just going to look at my papers because I've got Satoshi after my name,' he told me. 'I've got my little Satoshi mask on, and people go "Aren't you wonderful?" because you were Satoshi. I wanted the doubt. When I released future papers, I wanted people to go: "Oh, fuck, he could be, and these papers are so good he might be."'

Dave Kleiman was to become the most important person in Wright's professional life, the man he says helped him do Satoshi's work. They met online: they visited the same cryptography forums and had interacted since 2003. Both men were interested in cyber security, digital forensics and the future of money, but Kleiman was a boy's boy, an army veteran who loved contact sports and fast living. Five foot ten and weighing 200 pounds, he lived in Riviera Beach, Florida, and from 1986 to 1990 he was an army helicopter technician. When I looked into Kleiman's life, I discovered he had also done computer forensics work for Homeland Security and the army. After active service he became a deputy in the Palm Beach County sheriff's office. A motorcycle crash in 1995, when he was 28, left him in a wheelchair. Kleiman was a drug user and one source told me he was heavily into online gambling and various illicit activities; there is evidence he was associated with Silk Road, the online marketplace for all things illegal. After the accident he devoted himself to computers, and set up a company called Computer Forensics LLC.

Until Napster (the brainchild of a teenager called Shawn Fanning) came along in 1999, enabling users to share music files across the internet without a central server, the phrase 'peer-to-peer sharing' was familiar only to the early internet's true believers. Napster, with its user-friendly interface, brought file-sharing to the

masses. The old model of copyright and revenue generation became obsolete overnight: people stopped buying CDs; young people got music through the internet for free. The music industry had to reinvent itself or die. Wright told me that his earliest conversations with Kleiman were about file-sharing. In 2007 they wrote a study guide together on hacking. ‘I used to fire ideas off him,’ Wright said. ‘I’m pretty good at maths but I’m not very good at people.’ Kleiman, he said, could put up with his temper, which not everybody could. They began to speak of ways to use the Napster idea in other areas and solve some old problems in cryptography. Wright never, I have to say, made it fully clear how they had collaborated on building bitcoin. I kept returning to the subject, and my doubts would flare up when he failed to be explicit.

‘Give me a sense of how the idea of Satoshi formed,’ I said.

‘I guess,’ Wright replied, ‘the initial idea was having a pseudonymous head that wouldn’t be cut off.’

‘More your idea than his?’

‘Probably mine.’

‘And was there a point you realised you needed a figurehead?’ I asked.

‘We needed people to respond to us,’ he said. ‘But I didn’t really want people to respond to me. There are a couple of reasons for that. I don’t think I would really have sold the idea to anyone. If I’d come out originally as Satoshi without Dave, I don’t think it would have gone anywhere. I’ve had too many conversations with people who get annoyed because it’s me.’

‘The blockchain came about as an idea of a ledger,’ he said. ‘But there were a number of problems that needed to be solved. It needed to be distributed, but how do you make sure people don’t collude – it may seem awful but you don’t put trust in people, you incentivise people to act. And you incentivise people to act by giving them the opportunity to earn something. It’s as Adam Smith says: it’s not through the goodness of the heart, it’s not the baker caring about you, it’s not the butcher

caring about you, it's them caring about their own families. Together, as he put it, the invisible hand controls the way society works.'

I asked him to explain the distributed ledger in layman's terms and he went into an algorithmic paroxysm of verbal ingenuity. Ignoring all that, a distributed ledger is a database that is shared between multiple users, with every contributor to the network having their own identical copy of the database. Any and all additions or alterations to the ledger are mirrored in every copy as soon as they're made. No central authority is in charge of it, but no entry on it can be disputed. Adam Smith's point about 'incentive' is embedded in the way bitcoin works: people do not just buy coins or use them; they 'mine' them. Miners use their computers to solve increasingly difficult mathematical problems, the reward for the solving of which can be paid in bitcoin. This keeps the currency honest and, ideally, stops it from being dominated by any single entity.

I had brought rolls of disposable whiteboard and stuck it up around the flat, and, while we were speaking, he would jump up and cover the walls in formulae, along with arrows, arcs and curves. His wife told me she sometimes goes into the shower room and finds him standing there, stark naked, writing on the steamed glass. 'Was there a primary person doing the maths?' I asked.

'Me,' he said. 'Dave wasn't really a mathematician. What he did was make me simplify it.'

'How did he know how to make you simplify it?'

'We got to a point in the writing of the Satoshi white paper where it was … People say that it was hard.'

'He wanted you to bring the language down a little bit?'

'A lot. It's very simple. The elliptical curve stuff is not described in the paper at all, it's just there. The crypto stuff isn't described either.' I asked him to show me the

trail of ideas that led to their collaboration. ‘So all these things are there,’ he said, pointing to a 337-page thesis on his computer called ‘The Quantification of Information Systems Risk’, which he had recently submitted in partial fulfilment of a philosophy doctorate at Charles Sturt University. ‘Application to audits, how you analyse failures, deriving the mathematics behind it, simplifying the mathematics and there you go … The core of the bitcoin paper is a Poisson model based on binomial distribution. That’s how it got solved.’

In 2008 it was a ‘hodgepodge’, he said. I asked him if he felt the development of bitcoin was, at some level, a response to the financial crisis. ‘It was already in process. I saw [the crisis] coming though. It was a kind of perfect storm. During that year, I spoke to Wei Dai. So between him and Hal Finney there were a lot of really good ideas about making money work … [Finney] was the one who actually took what I said seriously. He received the first bitcoin.’

Craig started turning up to our interviews in a three-piece suit. His suits were unfashionable and his ties even more so – 1970s-style yellow, sometimes paisley – and he would ramble on a range of subjects. On his own subject, he could be brilliant, but he was wayward: he would side-track, miss the point and never come back to it. He was nothing like people imagine the mythical Satoshi to be – in fact, he was Satoshi’s comic opposite. He told stories against himself that weren’t really against himself. He was obsessed with his opponents’ views but had no skill at providing a straight answer to their questions. ‘I’m an arsehole,’ he said many times, as if saying so were a major concession. But he wasn’t really, he was actually pretty nice. He was arrogant about maths and computing, which wasn’t so surprising. He also had a habit of dissembling, of now and then lying about small things in a way that cast shade on larger things. At one point, I asked him to send me an email from the original Satoshi account.

‘Can you do that?’ I asked.

'Yes,' he said. 'But I'd need Rob's permission.' When I asked MacGregor he said that was absurd. He simply didn't want to – or couldn't – give too much away, and that was unfortunate in someone who'd agreed to sit down every day with a writer. He seemed to have full knowledge of that email account, in a way that made it seem unquestionably his. But somehow, it offended his sense of personal power to prove it. At first, I thought he was a man in existential crisis, like the hero of Bellow's *Dangling Man*, brilliant but antisocial, waiting to be drafted. But as the months passed I began to think of him more as a Russian 'superfluous' man of the 1850s, a romantic hero out of Turgenev, constantly held back from self-realisation by some blinding secret, showing himself not by action but in speech. Wright talked all day and he scribbled on the board and he called me his friend. He cried and he shouted and he unloaded his childhood and spoke about his father. He claimed to be Satoshi and he spoke Satoshi's thoughts and described what he did and gave an account of what people misunderstood about his invention and where bitcoin needed to go now. I moved to an office in Piccadilly – it was like something out of John le Carré, all those rooftops and fluttering Union Jacks – and we continued to do interviews. He talked without cease, without direction, and continued to find it difficult to land near the spot where my question was marked on the ground. When I asked to see the emails between him and Kleiman, he shrugged. He said he wasn't getting on well with his first wife when he wrote them and I assumed that meant they were full of talk about her. 'Just edit them down for me,' I said.

'I don't know if I can find them,' he said. But I wouldn't let it go and eventually he sent me a selection and they certainly seem to be authentic. A few of the emails were obviously the same as those quoted in the *Wired* and *Gizmodo* stories before Christmas. Wright always said these stories had been provoked by a 'leak', the work of a disgruntled employee of his who had stolen a hard drive. In any case, the emails he sent me show a pair of men with shadowy habits – socially undernourished men, I'd say, with a high degree of intellectual ability – operating in a world where the line between inventing and scamming is not always clear. The first email Wright sent me was from 27 November 2007, when he was working for

the Sydney accountancy firm BDO Kendalls and the two men were working on a paper on ‘Cookies in Internet Banking’. ‘Next year Dave, we come out with something big. I will tell you, but not now,’ he wrote to Kleiman on 22 December 2007. Kleiman’s reply told him what he was reading – ‘Sagan, Feynman, Einstein’ – and added: ‘I hope we make an event together this year so we can “break some bread” and have a casual conversation, instead of the brain dump middle of the night email exchanges we normally have.’ On 1 January 2008, Wright closed an email: ‘Nothing now, but I want your help on something big soon.’

The subject of bitcoin came up – quite starkly – in an email from Wright dated 12 March 2008. ‘I need your help editing a paper I am going to release later this year. I have been working on a new form of electronic money. Bit cash, bitcoin … you are always there for me Dave. I want you to be part of it all. I cannot release it as me. GMX, vistomail and Tor. I need your help and I need a version of me to make this work that is better than me.’ Wright told me that he did the coding and that Kleiman helped him to write the white paper and make the language ‘serene’. With a protocol as clever as the one underlying bitcoin, you would imagine the work was complex and endlessly discussed. But Wright says they mainly talked about it by direct message and by phone. Wright had been fired from his job at BDO (the crash was taking effect) and had retired with his then wife, Lynn, and many computers to a farm in Port Macquarie. It was there, Wright says, that he did the majority of the work on bitcoin and where he spoke to Kleiman most regularly. The Satoshi white paper, ‘Bitcoin: A Peer-to-Peer Electronic Cash System’, was published on a cryptography mailing list on 31 October 2008.

On 27 December 2008, Wright wrote to Kleiman: ‘My wife will not be happy, but I am not going back to work. I need time to get my idea going … The presentation was good and the paper is out. I am already getting shit from people and attacks on what we did. The bloody bastards are wrong and I friken showed it, they should stick to the science and piss off with their politicised crap. I need your help. You edited my paper and now I need to have you aid me build this idea.’ Wright told me

that it took several attempts to get the protocol up and running. He began to test it early in January 2009. ‘That was where the real money started rolling in,’ he told me. The originating block in the blockchain – the file that provably records every transaction ever made – is called the Genesis block. ‘There were actually a few versions of the Genesis block,’ Wright told me. ‘It fucked up a few times and we reviewed it a few times. The Genesis block is the one that didn’t crash.’ There from the beginning was Hal Finney, who would receive the first bitcoin transaction, on block 9. This was a key moment for the new cryptocurrency: block 9 for ever shows that Satoshi sent Finney ten bitcoin on 12 January 2009 – it is the first outgoing transaction we know to have come from Satoshi. Satoshi also sent four other transactions on the same day. I asked Wright who the recipients were – who the four addresses belonged to. ‘Hal, Dave, myself,’ he replied. ‘And another I cannot name as I have no right to do so.’ Wright told me that around this time he was in correspondence with Wei Dai, with Gavin Andresen, who would go on to lead the development of bitcoin, and Mike Hearn, a Google engineer who had ideas about the direction bitcoin should take. Yet when I asked for copies of the emails between Satoshi and these men he said they had been wiped when he was running from the ATO. It seemed odd, and still does, that some emails were lost while others were not. I think he believed it would be more interesting to play hide and seek than to be a man with a knowable past.

Wright’s emails to Kleiman suggest that by this point he was starting to mine the million or so bitcoins that are said to be owned by Satoshi Nakamoto. ‘I have a few potential clients in gaming and banking,’ he wrote to Kleiman. ‘I figure I can work ten to 15 hours a week and pretend to have a consultancy and use this to build and buy the machines I need. If I automate the code and monitoring, I can double the productivity and still offer more than others are doing … The racks are in place in Bagnoo and Lisarow. I figure we can have 100 cores a month setup and get to around 500.’ Kleiman replied the same day to affirm their vows.

‘Craig, you always know I am there for you. You changed the paradigm that was held for over a decade and destroyed the work of a couple [*sic*] academics. Do you really think they will just take this happily? I know you will not, but try not to take the comments to heart. Let the paper speak for itself. Next time you need to get me a copy of the conference proceedings as well. You know it is not easy for me to travel.’ A picture emerges of an ailing Kleiman sitting at his computer day and night in his small ranch-style house in Riviera Beach, Florida. After writing this last email, he spent a frighteningly long period in hospital. The two men agreed to meet up at a conference in Florida on 11 March 2009 and Kleiman wrote expressing his excitement at the prospect of a few beers with Wright. Craig and Lynn stayed at Disney’s Coronado Springs Resort Hotel and Kleiman drove there in his customised van, rolling into the bar with a big smile: Kleiman was the brother and drinking buddy and like-minded computer nerd Wright had never had. Not even Lynn had a clue what they were talking about.

During my visit to Australia I met Lynn in Chatswood, on Sydney’s north shore, a busy commercial district that heaves with eager shoppers on a Saturday morning. She had met Wright on the internet while she was working as the nursing manager of the ICU in a military hospital in Ottawa. She told me Wright asked her to marry him about six weeks after they met online. When she eventually went to Sydney to visit him, he brought a ring to the airport. ‘He was 26 and I was 44,’ she said. Neither of them had been married before.

‘He was very mature for 26,’ Lynn told me. ‘He always has to be the best. And the hard part about that is he left bodies by the wayside. He stepped on people.’ She began working for him – ‘he was the geek and I was the gofer’ – and he got a lot of work in information security, working for the Australian Securities Exchange, and Centrebet, which is where he first got to know Stefan Matthews. Wright told me he was afraid some of the things he did for those online betting companies would come back to bite him, if and when he was outed as Satoshi. Other sources told me that he and Kleiman had had some involvement with illegal gambling. ‘I knew Dave

Kleiman and he were working together,' Lynn told me, 'and I remember them saying that digital money was the way of the future. I've never said this to anybody, but I knew he was working on it and I didn't ask, because I knew he would bite my head off if I didn't understand it. He's got a very sociopathic personality.'

Lynn said her husband had admired Kleiman. And she admired him too: 'He loved life,' she said, 'and he had a brilliant mind, like Craig, but he had a gentler soul.' She remembered the Orlando conference. 'We stayed in a hotel that looked like a giant cartoon,' she told me. 'We met in one of the bars. He was a young guy, in his thirties or early forties, brown hair and moustache, average-looking. And boy, he loved to have a good time. It might have been his birthday. I went into the Disney store and bought some hats – Craig had Pluto, and Dave had one in the shape of a giant birthday cake.' Wright stepped out of himself for Kleiman: 'I'd never seen him like that with anybody. It was like, "I wanna grow up to be just like him." Dave softened Craig. A lot of what they wrote together was in his voice. I'd never seen Craig react like that to anybody. When he felt unsure of himself he went and talked to Dave. I think he wanted to be like Dave, but he knew he couldn't be.'

'In terms of having that kind of temperament?'

'Yeah. Dave was good for him. It made him realise that life doesn't go your way all of the time.'

I asked her if she thought he was a flawed person. 'Yes,' she said. 'He's starting to realise it. He knows he's done well in his work but he hasn't done well as a human being.' She stared into her cup. 'When we were at the farm,' she said, 'I was interested in finding four-leaf clovers. I would never find any, but Craig would just step out of the house and find three.'

In mid-2011 Satoshi suddenly disappeared from view. Apart from one or two emails denouncing fake Satoshis, he wasn't heard from again. Control of the network alert key is said to have been passed at this time to Andresen – possession of this key

makes its holder the closest thing bitcoin has to a chief. Wright sent Kleiman an email on 10 September 2011: ‘It is recorded. I cannot do the Satoshi bit any more. They no longer listen. I am better as a myth. Back to my lectures and rants that everyone ignores as me. I hate this Dave, my pseudonym is more popular than I can ever hope to be.’

For some reason – possibly fear of the ATO – Wright set up a trust fund called the Tulip Trust in June 2011, and asked Kleiman to sign an agreement stating that he, Kleiman, would hold 1,100,111 bitcoin (then valued at £100,000, currently worth around $800 million). For clarity: there is no evidence that Kleiman ever took custody of that amount. However, there was a separate agreement that Kleiman would receive 350,000 bitcoin and this transaction was made. ‘All bitcoin will be returned to Dr right on 1 January 2020,’ it says in the trust document.

> No record of this arrangement will be made public at any time … Dr Wright MAY request a loan of bitcoin for the following reasons (and no others): Furthering research into peer to peer systems … commercial activities that enhance the value and position of bitcoin. In all events, all transactions in loaned funds will be concluded outside of Australia and the USA until and unless a clear and acceptable path to the recognition of bitcoin as currency has occurred … I lastly acknowledge that I will not divulge the identity of the Key with ID C941FE6D nor of the origins of the satoshin@gmx.com email.

Kleiman signed it. ‘I think you are mad and this is risky,’ he wrote in an email to Wright on 24 June 2011, perhaps spying a possible illegality. ‘But I believe in what we are trying to do.’ Wright meanwhile seemed to get more and more frustrated. He both wanted fame and repudiated it, craving the recognition he felt was his due while claiming his only wish was to get back to his desk. ‘I have people who love my secret identity and hate me,’ he wrote to Kleiman on 23 October that year. ‘I have hundreds of papers. Satoshi has one. Nothing, just one bloody paper and I cannot associate myself with ME! I am tired of all these dicks Dave. Tired of academic attacks. Tired of tax fuckwits. Tired of having to do shenanigans like moving stuff overseas IN CASE it works.’

I came to feel that there were secrets between Wright and Kleiman that might never be revealed. Wright usually clammed up when asked about Kleiman and money. One day, in a fit of high spirits, he showed me a piece of software he said that US Homeland Security had ripped off from him and Kleiman. He smiled when I asked if they'd done government security work. The first thing most people ask about when you mention Satoshi is his alleged hoard of bitcoin: he invented the thing, and created the Genesis block, and mined bitcoin from the start, so where was Wright's money and where was Kleiman's? The emails, when I got them, seemed to clear this up slightly, but, during many dozens of hours of conversation with Wright, he never properly told me how many bitcoin he mined. I was aware – and he knew I was aware, because I told him several times – that he wasn't giving me a full account of everything that had occurred between him and Kleiman. He said it was complicated.

Somewhat more helpful are minutes taken during a meeting between the ATO and representatives from Wright's Australian companies in Sydney on 26 February 2014. According to the minutes, Wright's representative John Cheshire went into detail about the financial collaboration between Wright and Kleiman. This was a story that Wright, for some reason, didn't want to tell me. Cheshire said that Wright and Kleiman had set up a company called W&K Info Defense LLC (W&K), 'an entity created for the purpose of mining bitcoins'. Some of these bitcoins were put into a Seychelles trust and some into one in Singapore. Wright, according to Cheshire, 'had gotten approximately 1.1 million bitcoins. There was a point in time when he had around 10 per cent of all the bitcoins out there. Mr Kleiman would have had a similar amount.'

I asked Wright about this and he told me it was true that his and Kleiman's mining activity had led to a complicated trust. The trust question was persistently vague: not only how many trusts but the names of the trustees, and the dates of their formation. The only consistent thing is the amount of bitcoin Wright is said to have had at one time, 1.1 million. He said that his bitcoin could not now be moved without

the agreement of the (several) trustees. He also said that Kleiman had been given 350,000 bitcoin but had not moved them. He kept them on a personal hard drive.

Wright also set up a shell company in the UK. ‘I know what you want and I know how impatient you can be,’ Kleiman wrote on 10 December 2012, ‘but really, we need to do this right. If you fail you can start again. That is the real beauty of what you have.’ It’s possible Kleiman was referring to their ability to mine bitcoins and then squirrel them away. But he was evidently worried about Wright’s ability to cope with all the flak, and about Wright’s kamikaze attitude to the tax authorities. ‘I love you like a brother Craig,’ he added, ‘but you are a really difficult person to be close to. You need people. Stop pushing them away. You have over one million bitcoin now in the trust. Start doing something for yourself and this family you have.’

Around this time, an 18-year-old IT enthusiast called Uyen Nguyen began working with them. Very quickly, Kleiman made her a co-director of their company and she later became a powerful figure in the trust. It’s unclear how such a young and inexperienced person came to have so much influence. Wright told me she was ‘volatile, capricious and beyond control’ and added that Kleiman liked young women and that she was loyal and trusted – but that ‘she wants to help and this always leads to trouble.’ While I was preparing this story, Wright began to seem worried about Nguyen. I always felt he was in the middle of a very complicated lie when he talked about her. ‘**My way of lying**,’ he told me one day, ‘is to let you believe something. If you stop questioning and then you go off, and I don’t correct you – that’s my lie.’

Towards the end of 2012, Dave began to fail. ‘Paraplegics get sick a lot,’ Lynn Wright had told me, speaking as a nurse. ‘The bedsores get bad and they can’t fight infections. Dave was in and out of hospital a lot and I don’t know what his life was really like.’ Wright told me that Kleiman had girlfriends, but admitted he didn’t really know much about his life. Like Wright and his first wife, they had met in a chatroom. They met in the flesh no more than half a dozen times. Kleiman seems to have lived in front of his computer day and night, and the sicker he got the more isolated he

seemed to be. Just after 6 p.m. on 27 April 2013 he was found dead by a friend who'd been trying to contact him for several days. He was sitting in his wheelchair and leaning to the left with his head resting on his hand. Lying next to him on the bed was a 0.45 calibre semi-automatic handgun, a bottle of whisky and a loaded magazine of bullets. In the mattress a few feet from where he sat, a bullet hole was found, but Kleiman had died from coronary heart disease. There were prescription medicines in his bloodstream and a modest amount of cocaine.

'We never really thought that "we made Satoshi,"' Wright told me once. 'It was good. It was done. It was cool. But I don't think we realised how big it would be.'

'There was no conversation between you about how it was going over? That Satoshi was becoming a guru?'

'We thought it was funny.'

Wright paused, shook his head, and broke down. 'I loved Dave,' he said. 'I would have seen him more. I would have talked to him more. I would've made sure he had some fucking money to go to a decent hospital. I don't think he had the right to choose not to tell me.'

'What was happening to him?'

'Neither of us had any money, physical money. We had money in Liberty, an exchange in Costa Rica, but the Americans closed it down as a money-laundering operation. Dave had a number of bitcoins on the hard drive he carried with him. Probably about 350,000.'

'Hoping it would …'

'As I said, it wasn't worth that much then. Dave died a week before the value went up by 25 times.' Wright kept wiping his eyes and shaking his head. He emphasised something he said the commentators never understood: for a long time, bitcoin

wasn't worth anything, and they constantly needed money to keep the whole operation going. They feared that dumping their bitcoin hoard would have flooded the market and devalued the currency. One of the things Wright and Kleiman had in common is that they had a problem turning their ideas into cash and were always being chased by creditors. Kleiman died feeling like a failure. No one in his family has the passwords to release the bitcoins on his computer. After he died, his family didn't open probate on his estate because they believed it had no value. Kleiman's supposed personal bitcoin holdings are worth $260 million at today's prices.

**The London Office**

In January this year, on a rainy London afternoon, Wright took me to see the large office that was being set up for him as part of the deal with nCrypt. It hadn't taken long for the world to forget that they'd once thought Wright was Satoshi. One or two of the media organisations that had 'outed' him in December had taken down the original articles from their websites, stung by the cries of fraud. After only a few days' interest in the notion, most people had made up their minds that Wright had nothing to do with Satoshi. Wright – under strict advisement – had said nothing in response to the media reports accusing him of perpetrating a hoax, but when we were alone, which was most of the time, he would launch into point-by-point rebuttals of what his critics had been saying. In the end he would shrug, as if the most obscure things were actually obvious.

The press coverage of Wright and Wright himself had something in common: they succeeded in making him seem less plausible than he actually was, and, to me, that is a general truth about computer geeks. They are content to know what they know and not to explain it. They will answer a straightforward slur with an algorithm, or fail to claim credit for something big then spend all night trying to claim credit for something small. Many of the accusations of lying that were thrown at Wright last December were thrown by other coders. And that's what they're like – see Reddit, or any of the bitcoin forums. Much of what these people do they do in the dark, beyond scrutiny, and, just as it's against their nature to incriminate themselves, it is

equally unnatural for them, even under pressure, to de-incriminate themselves. They just shrug.

Coders call one another liars, when all they really mean is that they disagree about how software should work. During the time I was working with Wright in secret, I would text my colleague John Lanchester, who I knew I could trust to keep the secret but also to understand what was at stake in the story. ‘Imagine a situation,’ I wrote to John, ‘where novelists were strangely invested in denying the plausibility of each other’s books. There’s no “proof” as such that one is right and the other is wrong, but they could argue fiercely and accuse each other of all sorts of things while not really settling the problem.’

‘Edmund Wilson says somewhere that the reason poets dislike each other’s books is because they seem wrong, false – a kind of lie,’ John replied. ‘If you were telling the truth you would be writing the same poems as me.’

So the world that Wright knew best thought he was a liar. And the day we visited his new offices he seemed resigned to the fact. Much later, he told me that these months were the high-point of his career in computer science: he was working in secret on material that seemed to be coming together beautifully and profitably. It irked him that people called him a fraud and it irked him, just as much, that his deal with nCrypt would require him to prove that he was Satoshi. He hated being accused of being a fraud *and* he hated having to prove that he wasn’t a fraud. Having it both ways is a life, a life that requires a certain courage as well as shamelessness, and Wright was living his double life to the hilt.

Wright introduced me to Allan Pedersen, who’d been his project manager in Sydney. We were in the Workshop – a floor above MacGregor’s office near Oxford Circus – standing at a glass workbench beside a whiteboard covered in writing. The opposite wall was stencilled with a quote from Henry Ford: ‘Whether you think you can or think you can’t, you are right.’ Pedersen told me he had been brought over to direct a group preparing an initial batch of 32 patent applications, to be completed

by April. (This was in January.) Beyond that there were ‘upwards of four hundred patents’, ideas to do with using the blockchain to set up contracts that would come into action on specified dates years ahead, or using the blockchain to allow cars to tell their owners when they needed petrol and to debit the cost when they refuelled. At this point, and for several minutes afterwards, Wright spoke of himself in the third person. ‘Craig has been given a big kick up the bum,’ he said, ‘because Craig, instead of doing tons of research and sticking it on a shelf, has to complete it and turn it into something.’

‘How do you organise him?’ I asked Pedersen.

‘I’m the organised type,’ he said. ‘When Craig comes into the office he’s always in the middle of a sentence. And I’m trying to work out what this sentence is and manage things around what he’s saying. I’m sort of grounding his latest thoughts, placing them in what we’re trying to do. I’m the glue between Craig and the developers.’

It had become obvious, mainly from things Wright himself had said, that he often found it difficult to get on with people who worked for him. He got rattled when they said things couldn’t be done, or were too conventional in their thinking, or too stupid, as he saw it. Ramona told me that 40 per cent of his staff in Sydney had been in a state of rebellion. ‘I’m an arsehole,’ Craig said to me once again, ‘and I know that.’ Pedersen had the job of keeping things cool with the developers, whose job it was to turn Wright’s ideas into a form in which they could be patented and eventually licensed. ‘I’m making sure the ideas get executed,’ he said. ‘Craig’s not that interested in that part. He’s always moving on.’

‘Craig’s great at research,’ Wright said, ‘but his development and commercialisation sucks. I build it, and then it works, and then I walk off.’

‘You’re losing interest?’

‘I’ve lost interest. I’ve proved it, and off I go.’

‘It’s getting easier,’ Pedersen said, with a smile. ‘It was quite complex in the beginning.’ Wright had strong views about how the technology should develop, and how it could ‘scale’ to meet greater demand. ‘It can go to any size,’ Wright said that day. I’ve tested up to 340 gigabyte blocks, which is hundreds of thousands of times greater than it is now. It’s every stock exchange, it’s every registry rolled into one … Ultimately bitcoin is a 1980s program, because that’s what I was trained in … The idea is good, the code is robust, it runs and does the job, but it’s slow and cumbersome. There were some things early on that needed to be fixed and were, but it wasn’t as perfect as everyone thinks. At the end of the day, it needs to be turned into professional code. It needs to move away from the home user network and into a server network environment. And then it can do much more and be faster.’ There are those who feel it should remain small, and that making it bigger is a betrayal of its first principles.

‘This is the future of the blockchain,’ Pedersen said.

‘People are saying, “It’s not really something we can run yet,”’ Wright said, ‘but it’s time that we grew up and that bitcoin becomes professional.’

Pedersen shook his head. ‘We’re not working in a world where we know exactly what we’re doing,’ he said. ‘It’s coming from Craig. And then I start establishing the ground rules and we begin rolling it out. I’m putting people on a certain track and I keep going back to Craig, saying, “We need to sort this or that out,” and I’m constantly keeping them and him in the loop. The good thing about Craig is that he wants me to task him, so it’s a very strange relationship we’ve got. I’m reporting to him but I’m tasking him at the same time and it seems to work beautifully.’ He was tired, and so was the whole team, but they felt confident the patent applications would be filed on time.

When Craig left the room to take a phone call, Pedersen took pains to close the door properly. ‘He’s a really nice person,’ he said, ‘but he’s a fucking nightmare. Every single morning he comes in and I think, “What is he talking about?”’ Pedersen told me how he handled him, how he made him focus, and how he worked hard to keep him on track. ‘When I’ve got new people here,’ he said, and there were many new people, ‘I have to train them how to talk to Craig. That’s what I have to do. Sometimes, he can’t explain things and this is where the anger comes from. It’s the interesting part. You can’t be in the same room with him. He’s constantly telling you something. He’s like Steve Jobs, you know – only worse.’

As we made our way to the new office – it was a building site that day, but would be up and running four weeks later – Wright presented himself as a man who was ready for anything. In a pinstripe suit and ruby tie, he looked like a hellbent 1980s bond dealer, except the cypherpunk glint in the eye suggested he was getting away with something. He wasn’t the king of all he surveyed, he was the joker, and, crossing Oxford Street, he joked that he might be Moses. The traffic parted and he made his way to the promised land, a brand new suite of offices down a side street.

*

Pedersen had come along. ‘This is how it works in this company,’ he said. ‘You’re sitting in Vancouver in October’ – Vancouver is where nTrust, the parent company, is based – ‘and suddenly Rob MacGregor says: “We need these thirty-odd patents by April and when can you go to London?”’ The hurry for the patents was to help with the giant sale to Google or whomever. The men behind the deal were very keen to beat other blockchain developers to the punch, especially the R3 consortium of banks and financial institutions which late last year started spending a fortune trying to deploy the technology. We were accompanied by a young Irish woman who had been put in charge of designing the new office. MacGregor’s firm had invested millions in Wright. The new company, nCrypt, had pretty much been built around him, and its offices showed it. He was to have the enormous corner office with a view all the way along Oxford Street. MacGregor clearly believed in

Wright, however obnoxious he could be, but I never understood why he wasn't interrogating his uncertainties before spending his money. He was a lawyer, but he put trust in front of diligence, which is unusual in someone so intelligent. MacGregor never, incidentally, used the words 'off the record' with me – only once, later on, did he imply it, when he said something and then said he'd deny saying it if I quoted him – and he was a generous source of information. At no point, however, did he tell me where the money for this project was coming from.

The designer was waving a colour swatch. 'We've gone for a kind of Scandi look,' she said.

'This place will work,' Wright said, striding through the open space, 'mainly when it comes to protecting me from myself.' Amid the hammering and drilling, Wright stood in an office about 20 feet by 20 feet, with floor to ceiling windows and a view down into the heart of Soho.

'You remember J.R. Ewing in *Dallas*?' I asked.

Wright laughed. What he most enjoyed, he said, was that all this was going on in secret while the world outside had written him off as a mug and a fantasist. 'If Satoshi has to come out, he'll come out in style.' He turned back to the designer to tell her how the frosted glass should work in the meeting room. 'We do a lot of work on whiteboards,' he said. He pursed his lips, then smiled. 'Will the interactive whiteboards be set up so that I can contact the guys in Sydney?'

We spent an hour at the new office. 'And they say *nothing is going on*,' Wright said as we stepped back into the elevator. 'It's all a *figment of our imagination*. I'm not Satoshi, and none of this is real.' Out on the street again, he told me he had all the money he would ever need. 'And I'll have the monkeys off my back for ever and just get on with the one thing I'm good at, not business, not managing people, but doing research and honouring this thing we made.' Wright was enjoying himself, but nCrypt was already, as MacGregor told me repeatedly, negotiating the sale of the

whole package to the highest bidder: ‘Buy in, sell out, make some zeroes,’ as he had said, and he’d always been honest about that goal. Wright wasn’t facing up to this. The next time I visited his corner office it was finished and decked out with claret-red leather armchairs and sofas flown in from Sydney. It looked, as I’d joked earlier, like the office of a Texan oil magnate. A host of management certificates were framed on the wall next to a signed photograph of Muhammad Ali.

I told Pedersen I thought Wright was struggling with the fine print of the deal – coming out. ‘He’s sold his soul,’ Pedersen said. ‘That’s how simple this is. And the combination of Craig and Ramona is dangerous here. They can’t just sign all these [legal] papers and think it’s going to be all right, that they’ll sort something out. It doesn’t work that way. They now have to go to the end and live with it. But they’re doing it on first class. When this Satoshi thing comes out I can see a lot of bad things happening, and they are not geared up for this, any of them.’

‘I’m concerned for him,’ I said.

‘There’s not really a happy ending here,’ Pedersen said.

‘Was it the same in Australia?’

‘It was the exact same,’ he said, ‘except in Australia you could say he was in control. He’s learned absolutely nothing. He’s now in this box, he can’t move, he can’t do anything, and this box is getting smaller and smaller.’

‘Do you think he wants to be outed as Satoshi?’

‘Yes I do. It’s in in his personality. He wants to be recognised. He says too much. After two weeks of working with him, I knew.’

‘He and Ramona tell me they had a pact never to come out.’

‘My feeling is that she doesn’t want him to come out, but he does. He’s been pushing for this to happen.’

I spoke to one of the scientists, a shy, unexcitable man in his late fifties, who has been working on this technology for several years. He and Pedersen are old-school IT people, quiet-spoken and completely uninterested in the limelight. Both of them thought Wright was working at a different level from everybody else. The scientist, who spoke to me from the beginning on condition that he wouldn’t be named, worried about Wright’s attention to detail and about his conspiratorial nature, but he had no doubts about Wright’s command of the big picture. The scientist was helping to oversee all the white papers and patent applications and managing a large team of IT specialists and mathematicians. I asked him if he was worried about the R3 consortium’s work on blockchain technology. ‘They are going to fail,’ he said. ‘They don’t have Satoshi. There is a panic out there, a misunderstanding about how the blockchain and bitcoin works. They hire people who know about bitcoin and are attempting to buy into it rather than being left behind. I’ve read some patent applications that are pending, applied for by the Bank of America. What I saw was ultimately unimpressive in comparison to what Craig is trying to do with the blockchain.’

The scientist described how the staff try to get the ideas out of Wright’s head. ‘You can’t say: “Explain this to me.” If you ask a question like that, he’ll just go off on giant tangents. First, he’ll have difficulty explaining what’s in his head. Often he’s just coming up with ideas on the spot that he’ll throw into conversation. You want to try to get yes and no answers from him. We film him at the whiteboard and someone will type out the text.’

He described moments when everyone in the research team thought what Wright was saying was impossible. It couldn’t be done, the software wasn’t up to it, the blockchain couldn’t scale to the task, and then suddenly everyone would understand what he was saying and appreciate its originality. ‘I need to be able to go over what he’s said,’ the scientist told me, ‘to find the pearls of wisdom and find out what the

hell he means. If I don't get it then I might have to make some guesses. I had to train my team to work in that mode. They have to be good researchers. They have to *understand* the technology as well as be able to work with it.'

Often, the scientist said, the staff were amazed by an unexpected turn in Wright's thinking. But he admitted to being amazed, too, by certain gaps in Wright's technical knowledge. It was bizarre. Wright had what the scientist and the team regarded as vast experience and command of the blockchain, which he spoke of as his invention and appeared to know inside out, but then he would file a piece of maths that didn't work. Or he would show a lack of detailed knowledge of something the team took for granted. Nobody I spoke to could explain this discrepancy. 'One of the problems with him is that he's a terrible communicator,' the scientist said. 'He's invented this beautiful thing – the internet of value. But sometimes he'll just talk in equations but can't or is unwilling to explain their content and application.' His mistakes could also, he implied, be a result of laziness and lack of attention to detail.

I knew this for myself, but I was, to some extent, vexed that the technologists had the same experience. At the same time, I was impressed that people like the scientist and Pedersen could live with such a high degree of ambivalence about their boss. When I asked Pedersen if he thought the work was truly revolutionary, a non-native weariness came into his blue eyes. 'I think so,' he said. 'But I don't think he'll get the Nobel Prize because he's too political. He's coming out as a street fighter and could end up in prison or whatever.'

*

The main players in this story were keen to help me, to talk about what they knew and to show me the documents, but, in every case, there were topics they would avoid, and that were never cleared up. One of the most helpful individuals was Stefan Matthews. He pointed me in the direction of people from Wright's personal life, and sent me a typed history of his association with the man who would be Satoshi. Matthews noted that, when he signed the deal with MacGregor, Wright didn't have a feasible business plan for any of his companies. The Wrights' financial situation was dire. They couldn't pay their staff and a number had already left.

Pedersen and some others had stayed on without pay; Wright owed his lawyers $1 million. Superannuation remittances were overdue and loan repayments unpaid; the companies needed £200,000 just to make it to next week. Craig and Ramona had sold their cars. One of the companies was already in administration and, with the ATO closing in, 'all related entities were on the brink of collapse.' Before signing the deal, MacGregor, sources say, tried to assess the value of Wright's research, commissioning a 'high-level overview' of the companies. MacGregor instructed Matthews to be in Sydney on 24 June 2015, when a final appraisal of the businesses was undertaken and a draft arrangement negotiated for nTrust 'to acquire the intellectual property and the companies themselves'.

One night I went to have dinner with Matthews on my own. We met in the restaurant at the back of Fortnum & Mason, 92 Jermyn Street, and he seemed incongruous among the red banquettes – a large, bald Australian with a rough laugh and wearing a plaid shirt, keen to tell me everything he thought useful. Matthews seemed a much more affable character than MacGregor, both upfront and very loyal, without perhaps seeing how the two might cancel each other out. One of the tasks of the eager businessman is to make himself more sure of his own position, and Matthews spent a lot of time, as did MacGregor, selling the idea of Wright as Satoshi rather than investigating it. They drafted me into telling the world who Wright was, but they didn't really know for sure themselves, and at one point their seeming haste threatened to drive a wedge between us. It seemed odd that they would ask a writer to celebrate a truth without first providing overwhelming evidence that the truth was true. I took it in my stride, most of the time, and enjoyed the doubts, while hoping for clarity.

Matthews drank a little wine but not much. He was talking about the night in Sydney when they signed the deal. 'We pulled up outside Rob's hotel. He said: "Do you realise what you have just done? You have just done the deal of a career. This is a billion dollar deal. Fucking more. Billion dollars plus."'

'Why is Rob so convinced?'

‘Don’t know, don’t know.’ (MacGregor later told me he was convinced because Wright had shown Matthews the draft Satoshi white paper. ‘I always had that,’ MacGregor said.) ‘If it turns out that he’s a fraud, I don’t know how he’s managed to do it because you couldn’t make this up.’

Matthews told me about a meeting at the Bondi Iceberg Club in Sydney that Wright had with Ross Ulbricht, the founder of Silk Road, now serving two life sentences. Silk Road used bitcoin to trade all kinds of contraband items because the transactions could be made anonymously. Wright later confirmed that this meeting took place, but said only that Ulbricht was full of himself and they didn’t discuss bitcoin. Matthews seemed to think this was unlikely. He wondered whether Kleiman had had more to do with Ulbricht; other sources suggested the same.

‘Wright signed a deal to come out as Satoshi,’ I said to Matthews. ‘Does he realise everything that involves?’

‘You’re gonna have criminal groups that paid him lots of money and there are people who know about that,’ Matthews alleged. ‘If they quack? You’ve got Ross Ulbricht who’s in prison and apparently going to appeal trial this year or next. What happens when Ross sees Satoshi’s name splashed everywhere and Craig’s name everywhere? Is he going to say “I had lunch with that guy. We made a deal”? I’m not worried about what Craig has done, I worry about people who have associated with him.’ It was very strange to do an interview with someone who would come out with this stuff, given that he was also trying to market the guy. In fairness to Wright, Matthews might just have been running his mouth off, and I’ve left out the worst of what he said, now and later.

We talked about some of the difficulties that had arisen between Wright and MacGregor. ‘Craig and Ramona are in a state about the keys leaving the room,’ I said. ‘He feels it is an act of self-annihilation to let them go. Rob has a Hollywood ending in mind and it’s looking incredibly unlikely. You can’t go into a marketplace claiming full legitimacy when the proof hasn’t been produced.’ I told Matthews that

there were emails still missing between Wright and Kleiman, emails that the public would want to see before accepting him as Satoshi, because the correspondence would presumably go into the kind of detail about the invention that only the inventors could know. Wright had told me he would produce the missing emails by the following Wednesday, but he never did.

'I know what's in there,' Matthews told me. 'It will be chatter to do with illegal stuff that he and Dave were doing in Costa Rica – particularly around Costa Rican casinos where they got $23 million of income. And you don't get paid that amount just for doing a security review … He mined all those bitcoins himself using equipment that he bought with money that he got from Costa Rica.' Again: why was Matthews saying this? It was obvious to me that Wright was going to have a problem telling the full story, whatever it was. I wasn't even sure he'd told the full story to his wife, but perhaps he had, because she referred, several times, to the fact that there were things that she just couldn't tell me. 'They'll come after us,' she said, in a state of high emotion. 'They'll destroy us.' Matthews said he didn't know what that was about. He did tell me something he said he had told MacGregor when MacGregor asked him what he was getting out of the deal. 'Absolutely nothing,' Matthews said. 'I get what I get paid by Calvin. Calvin is the only allegiance I have, then and now.'

Calvin Ayre is one of the topics the team routinely went dark on. When I first met Wright, he called him 'the man in Antigua'. MacGregor never mentioned him at all during our early meetings. When I later told him that Ramona had mentioned a big man in Antigua, he said he didn't mind talking about him, but didn't bring his name up again. When, in February this year, they took Wright to Antigua for a pep talk, I emailed Matthews to ask if I could come too, and he didn't reply. Wright, in a low moment, later asked me if I'd told MacGregor they were the ones who let the cat out of the bag about Ayre. I said it wasn't them: Ayre's name had first been mentioned to me by Matthews. The Antigua meeting was being arranged when I went out for dinner with Matthews, and he referred to Ayre freely without ever asking that it be

off the record. MacGregor never went into detail about Ayre's involvement but both men's regular visits to Antigua made me wonder about the extent of the connection. Matthews, explicit as usual, always spoke about Ayre as if he was the *capo di tutti capi* of the entire affair, though I have no other evidence that Ayre was anything but an interested observer. Interestingly, nCrypt's only shareholder (one share worth one pound) is nCrypt Holdings, registered in Antigua.

Like MacGregor, Calvin Ayre is Canadian. His father, a pig-farmer, was convicted in 1987 of smuggling large amounts of Jamaican marijuana to Canada. When Calvin left college he went to work for a heart-valve manufacturer called Bicer Medical Systems and was later charged with insider trading, agreeing a deal where he was fined $10,000 and barred from running a public company listed on the Vancouver Stock Exchange until 2016. 'I clearly made some mistakes,' Ayre told the Vancouver *Sun*, 'but it was not a criminal issue and nobody got hurt from anything I did.' Ayre later started a software development company intended to help offshore betting companies take online bets. He relocated to Costa Rica in 1996, where he worked with two online casinos, WinSports and GrandPrix. Unlike most bookmakers, Ayre would send cheques directly, without using Western Union or an equivalent. He then set up Bodog, which would become the biggest name in the online gambling industry. (It's the company Matthews worked for after Centrebet.) Bodog was a huge success. In 2005, it handled more than $7 billion. Ayre appeared on the*Forbes* billionaires' list in 2006. In the same year, Bodog moved its global headquarters to Antigua. The IRS had started following the company in 2003 and US Customs and Immigration were also on his tail. A joint inquiry was started in 2006 and, in 2012, Ayre, along with two of the website's operators, was indicted on money-laundering charges. He entered no plea, but he maintains his innocence, seeing the indictment as 'an abuse of the criminal justice system'. In one profile of Ayre, we find him drinking coffee and paraphrasing Sun Tzu's *The Art of War*. 'I've put a lot of energy into finding ways not to fight my enemies,' he says. My researcher Josh showed me this interview, then remembered a note from my first meeting with MacGregor, in which he, too, had quoted Sun Tzu. 'You build your enemy a golden bridge to

retreat over,' MacGregor had said, drinking coffee. When he said this, I wasn't sure who the enemy was. The only person MacGregor had built a golden bridge for, so far as I knew, was Wright.

At the Jermyn Street dinner, Matthews didn't tell me any of Ayre's history, referring to him simply as a great guy. 'Do you know how many bitcoins Craig's got left of the original 1.1 million?' he asked later on. There are conflicting stories about the 'Satoshi millions'. Many people refer to a Satoshi-mined hoard that has never been spent, and the figure – always around a million bitcoin – is the same one admitted to by Wright and Kleiman. The difference is that Wright says he spent a lot of his. This was what Matthews was getting at. 'He told me last week,' Matthews said, 'and I've been having some sledgehammer conversations with Craig. I said to him: "Time for straight answers on this one, my friend. How many coins are left under the control of the Seychelles trust? And don't tell me you don't know because you're a grown man, and don't lie to me." And his answer was 100,000. I know that 650,000 was taken out to fund all the research and development stuff. And 350,000 is on Dave's hard drive. "Why has Dave got 350,000 of your coins on his encrypted hard drive?" Because he gave them to him. They're Dave's. Those wallets are encrypted on his hard drive, with three or four keys to his trust. Now, why did Dave die in squalor?'

'Why?'

'Because bitcoins weren't worth that much when Dave died. They skyrocketed around that time and in the weeks thereafter. But he was a man of principle apparently and wouldn't spend those coins unless Craig told him to.'

'And you don't think Dave mined coins himself?'

'Of course he did. No doubt. But how many? Who knows … We know they ran a business together based in Florida. They did stuff for contractors. We know that they lost money jointly in Liberty Reserve. And they would both have lost money in Mt Gox.'

Wright had told me he'd lost quite a bit when the bitcoin exchange Mt Gox was hacked and then collapsed. He also referred, in a later email, to information that was seeping from the collapsed Mt Gox database, some of it linking him to Ulbricht. 'The amount to a large wallet was me,' Wright told me. I took him to mean that there was evidence of a bitcoin transaction between him and Ulbricht. He wouldn't explain further.

As I was paying the bill, Matthews reared up. 'You know Craig has gone out and bought himself some cars? One hundred and eighty thousand dollars' worth of cars.' (When I checked this with Wright he said the cars were leased.) 'One of them stands out like the dog's balls in the proverbial moonlight, and this is from the man we're trying to keep fucking secret. How many custom BMW i8s are going around London? He's spending every fucking penny that we've paid him … Does he think this is just a game? You know, these guys have gone from being backyard scrappers and they've suddenly found themselves in a high-stakes poker game.' Matthews said he wouldn't take any rubbish from the Wrights, and that they'd end up on a plane back to Australia and jail if they didn't fulfil their end of the bargain, to reveal Satoshi. 'The people that I work with are capable of deciding this was a $30 million bad decision and write it off,' he said. I thought this a curiously revealing line, and wondered again just how he expected me to use such information.

'You haven't asked me why I'm doing this,' Matthews said at the end of the evening. He worked his way round to an answer, but it wasn't an answer, just more questions. 'Part of me,' he said, 'has asked over the past three or four months, why did I ever get involved in this? Why did Craig keep coming back to me? Why did he never shake out of my life? Why did he show me the Satoshi white paper in 2008? Why was he delivered back to me in 2015? I didn't go looking for it.'

*

Satoshi Nakamoto is not really a man; he is a manifestation of public acclamation, an entity made by technology, and a myth. Old-fashioned journalism might bring you

to him – or cause you to miss him altogether – but he was born of relationships that depend on concealment. A reporter was once a person who could rely on visible evidence, recordings, notes, statements of fact, and I gathered these assiduously, but this was a story that challenged the foundations on which reporting depends. I fought to uphold familiar standards of truth, and fought to discover new ways to uncover it in this underworld of companies with a vested interest in disclosing some things but not others, but it felt like the walls of virtual reality were forever pressing in on my notepad. It is standard practice in Silicon Valley for everyone, from bagel boy to research chief, to sign a Non-Disclosure Agreement. This is because every company – Apple or Microsoft or Google or Facebook – has a mission not only to make money but to control the narrative of who they are. A writer requires determination if he is to write anything about that world that isn't paid for or manufactured by a company. There is nothing particularly underhand about this: they offer you big money up front and ask you to sign over your allegiance. But when you turn down this offer and they don't banish you from the court, your version of reality might end up clashing with theirs. This happened several times during the months I was working on the Craig Wright story. Wright himself never mentioned rights or agreements or privacy – until the very end, when he asked for two particular aspects of his private life not to be discussed – but when I went to Australia at the end of February to talk with Wright's family and friends, the nCrypt men began insisting I sign an NDA.

Why they hadn't asked me to sign one at the beginning I'll never know. I had roamed freely for three months, noting and recording, going to meetings and interviewing everyone, and only now did they want me to sign. Early on, MacGregor told me in an email that he had advised Craig and Ramona to tell me 'everything'. He went on to express, on Wright's behalf, worries about how the material would be used. This was especially sensitive, I gathered, because of the government security work Wright had done. I replied that we would be judicious about what was published. MacGregor still wanted to discuss contractual issues, and I replied, on 6 March, that I would have to see proof that Wright was Satoshi, and see it presented

before his peers and selected journalists. MacGregor replied that the proof package was in train and that he didn't understand why I wouldn't sign. I replied on 7 March that I couldn't write the story, no matter how good my access, if there wasn't proof that Wright was Satoshi, and I was still waiting for evidence. 'My commitment is clear,' I wrote, 'but the book turns to dust if we do not have unanswerable and generous proof.' I insisted that I wouldn't sign any document and eventually MacGregor accepted this. We fell out over it, but I saw their point and I still do. Despite my refusal they continued, without binding agreements or legal constraints, to provide me with access to every meeting and every aspect of the story, which was set to change faster and in ways none of us could ever have prepared for. My story and nCrypt's deal seemed to be on the same track, aligned and friendly, but none of us discussed what would happen if the deal came unstuck.

**Proof**

When I asked Wright what kind of martial arts he did as a kid he gave the following answer. 'I did a few actually. I have studied in the Chinese forms Wing Chun, *Tánglángquán*, Kuo Shu, Duan Da, Zui Quan and *lóng xíng mó qiáo*. I have also mastered Muay Thai, Kenpo and Taekwondo and Chito-ryu style karate. I started with karate and Ninjutsu.' As with most things about him, it's not that it's not true, it just smells of self-doubt and a need not to hide anything positive about himself. It's the kind of truth-telling that expresses fear and gives rise to doubt, but it's not the same as a lie.

Wright's mother had told me about her son's long-standing habit of adding bits on to the truth, just to make it bigger. 'When he was a teenager,' she said, 'he went into the back of a car on his bike. It threw him through the window of a parked car. That's where his scar comes from. His sister accompanied him to the hospital and he's telling the doctor that he's had his nose broken twenty or so times, and the doctor is saying "You couldn't possibly have had it broken." And Craig says: "I sew myself up when I get injured."' What his mother said connected with something I'd noticed. In what he said, he often went further than he needed to; further than he

ought to have done. He appeared to start with the truth, and then, slowly, he would inflate his part until the whole story suddenly looked weak.

In the time since I'd last seen Matthews, he and MacGregor had been to Antigua with Wright and had agreed a 'proof strategy'. I had been pushing hard for the proof, and Ramona had asked me several times what Wright could do to prove to me that he was Satoshi. MacGregor asked the same thing during a meeting I attended with him and the public relations firm they'd hired, the Outside Organisation. 'It's not about proving it to me,' I said. 'It's about proving it – full stop. You just prove it for the whole world to see and then everybody goes home.' The nCrypt guys, pointing out that they had always intended to set up a proof session, organised a series of events with the help of the PR company, intended to bring Satoshi into the open. Originally, the plan was for the London School of Economics to host a panel discussion about the evidence and the findings, but someone seems to have blabbed to the *Financial Times*, which ran an article on 31 March. 'After nearly four months of silence,' the *FT* blogger Izabella Kaminska wrote, 'and a bitcoin community mostly resigned to the notion that the story was an elaborate hoax – conditional approaches are being made to media and other institutions in connection to an upcoming "big reveal" of Wright as Satoshi Nakamoto.' Her source was clearly inside the project. 'Wright will publicly perform a cryptographic miracle which proves his identity once and for all,' she wrote. MacGregor was outraged, and the LSE was sacked from the project. But the first and biggest of these proofs was to involve Wright using Satoshi's private encryption keys in sessions with key members of the bitcoin community. Jon Matonis, former head of the Bitcoin Foundation, agreed to take part. So did Gavin Andresen, one of the most respected bitcoin core developers, someone who had been there since its inception. These proof sessions would begin the denouement of this search for Satoshi.

Just before these sessions took place, in April, I asked Wright what had happened in Antigua. 'We discussed the whole PR strategy,' he said. 'The truth thing is going to happen.' He talked about Matonis and Andresen. 'We're going to bring them in on

reveal sessions in the next few weeks. I guess that's the way it has to be. Do I like it? No. But I haven't really been given a choice. I'm between a rock and a hard place because of whoever outed me last year.' He said very clearly at a meeting with me that he would not sign with the key in public. We agreed that he would do it for me at home, signing with the private key from one of Satoshi's original blocks. He would do for me what he was going to do for Matonis and Andresen, and this would prove beyond doubt, he said, that he was Satoshi. We made a plan, then Wright asked me to come to his office so he could draw something for me on his whiteboard, a new timelock encryption scheme he'd come up with. He wanted to add it to the list of patent applications. I didn't always know what he was talking about, but his expertise in certain areas was startling, and so were his obfuscations.

*

It was exactly 9 a.m. when I turned up at his house in South London, on one of those clear mornings when the planes leave trails in the sky. I knew his house by the BMW in the driveway, and I pressed the bell. He opened the door and a cloud of cologne came to meet me. In his study, there were three computers and seven screens. *Options, Futures and Other Derivatives* by John C. Hull was sitting on a grey sofa. There were rows of computing books and seven dead laptops stacked on top of a bookshelf. Even after all these months, Wright couldn't really do small talk, finding it hard to summon anything easy in himself. I asked him about his sofa and told him about a pain in my shoulder and he just said: 'Very good.' He made me a cup of tea and then beckoned me over to his main computer: it was time for him to prove to me that he was Satoshi. His manner was still that of a man who mildly resented having to prove anything. He smiled and pointed to the screen. 'This is his wallet, which is open,' he said. I saw a list of transactions with addresses specified. 'The initial Genesis block was hardcoded,' he said. 'There are no conflicting Genesis blocks. If a piece of code crashed on this machine it would still start on another machine with the same Genesis block. Always.' As I was looking at the screen in front of me and watching his hand move the mouse, lines from the

Wikipedia entry on the blockchain came into my head. ‘The blockchain consists of blocks that hold time-stamped batches of recent valid transactions. Each block includes the hash of the prior block, linking the blocks together. The linked blocks form a chain, with each additional block reinforcing those before it.’

‘It can’t be moved or changed?’

‘No. It’s hardcoded into the original program,’ he said.

Everything on his screen was time-stamped. I was looking at transactions from early January 2009. ‘I was officially canned from my job at BDO on 3 January,’ he said. He told me he went to his house at Port Macquarie and settled down to do the final work to get the bitcoin software up and running. ‘The original definition was published by Satoshi Nakamoto in 2008 and implemented in the original source code of bitcoin published in 2009,’ the Wikipedia entry said. As he explained what was in front of me, he clicked through the sequential blocks, the transactions database that underlies bitcoin. He was looking at the very earliest ones and all included dates, amounts of bitcoin and addresses. A long list of transactions showed incoming small amounts to Satoshi’s wallet. ‘Lots of people send micro payments to me,’ he said. ‘They think so much of Satoshi that they want to burn their pennies.’

‘So these fans are sending tiny payments to that known address? It is the first generated and the first known address?’

‘Yes. They’re hoping I’ll do something – out myself.’

The address was 12c6DSiU4Rq3P4ZxziKxzrL5LmMBrzjrJX. I could see that people had left messages – ‘public notes’ – for Satoshi: ‘Hey satoshi, change my life, send me some bitcoins!’ ‘God bless you, China.’ ‘If you are reading this, please take some time to remember those who died 12 years ago today in the WTC attacks.’

‘The bitcoin blockchain can be used as a trusted timestamp for arbitrary messages,’ Wikipedia said.

If you scroll back to the very first transaction associated with this address – 12c6DSiU4Rq3P4ZxziKxzrL5LmMBrzjrJX – you find that it is the first bitcoin transaction recorded. It was for 50 bitcoin and remains unspent. Anyone can enter that bitcoin address into a search engine and inspect the history of transactions associated with it. ‘The Genesis block was hardcoded on 3 January 2009,’ Wright said to me, ‘and that was the first run. There was no previous block.’ (Under the heading ‘Previous Block’, there is a line of 74 zeros.) ‘Then the code was reworked,’ he continued, ‘and fired up and the first address that was ever created from the hardcoded Genesis block – the first mined address – is the one I’m sending you a message from.’ He was about to use the original cryptographic key to sign a message to me and it was as if he was dropping a sugar lump into my tea. He typed the words, ‘Here I am, Andrew,’ and rested his fingers. ‘This gives us that little block there,’ he said, before verifying the signature. He looked sheepish and resigned in his blue checked shirt. ‘Welcome to the bit I was hoping to bury,’ he said. He leaned back and I noticed a samurai sword by the desk.

I shook his hand. Then I stared at the screen and considered how strange it would be to live with a secret for seven years and then feel no relief when it finally came out. Perhaps it never felt like a professional secret; it felt like a part of his being, and now he was giving it up. ‘I want it in layman’s terms,’ I said. ‘Explain what you just did.’

‘I just digitally signed a message using the first ever mined address on bitcoin.’

If he had done what he appeared to have done, and what he said he’d done, then his claim to be Satoshi was strong. For a moment, the amassed unlikelihoods and dissemblings seemed circumstantial, and the case against him suddenly much more fanciful than the idea of him being the famously secret man who invented this protocol. An alternative Satoshi would have had to share his entire password hoard

with him, and synchronised his 'real world' timeline in order to be placed where Wright was placed and align with his email existence and his expertise. It wasn't merely that Wright had been in the right place at the right time: he had been in the only place at the only time, and that time was stamped not only into the blockchain but into his correspondence and the experiences of those around him. He sat back in his large black chair and asked me if I wanted more tea. 'I could have been working with Satoshi, I guess,' he said, 'who told me he was going to fire it up at this time and I had all my machines ready and just took over from him. But that would make me Satoshi anyway.' He stared into the bank of screens and seemed nostalgic for a more ghostly self, and I asked him if it felt overwhelming.

'I don't care – whatever,' he said. But of course he did care – care is what he did most. He was agitated through the whole process, mainly, I guessed, from an old cypherpunk embarrassment at having to bend to authority. He wasn't satisfied when he sat back in his chair, he was annoyed and already making his detractors' arguments for them. 'They'll say I killed Satoshi and stole the keys. Having them doesn't prove I created them. Maybe it was a collaboration between me, Dave, Hal and some random person. Maybe I compromised Hal's machine and stole everything and his family didn't know. Maybe, maybe, fucking maybe. All that bullshit. Those people don't believe in Occam's razor. I've seen Reddit. They want the most convoluted explanation. But they can say what they want; I've got nothing more to prove.'

There is a message embedded in the Genesis block, a headline from the *Times* of 3 January 2009, the day the block was mined: 'Chancellor on brink of second bailout for banks.' I later asked Wright why he'd chosen that particular headline. 'As you know, I am rather anti-central/reserve bank,' he wrote to me. 'I see them as the true cause of these issues and the bubbles and collapses. But the date was important as a timestamp. It means that I could not have been "pre-mining" and gaming the system. The first iteration of the code was *finalised* on 9 January 2009. The run was started when I was at the farm in Macquarie later that week. It means that I cannot have been mining for months ahead and had collected a pre-mined set of solved

hashes to game the system. I ran more than fifty machines, so the headline was a marker.'

The question of proof in a story about computer science is a question for the birds. If you can't check the maths, how can you be sure? I wrote to four Princeton and Stanford cryptocurrency experts during the preparation of this story and sent them some of Wright's white papers. These men, who are together about to publish a textbook on bitcoin and blockchain technology, are obsessed with who Satoshi is, and obsessed with who he isn't. But they behave like visitors to a funhouse: they see distorting mirrors everywhere and hear distant laughter and weird music. Some of them did want to see the evidence, but they didn't want to be seen responding to it and I never heard from them again. And that is the kind of attitude that pervades the not entirely adult world of new inventions in the highly contested world of computer science.

Another thing: when such people want to make a point, they often want to destroy those they disagree with. It's clear how paranoia-inducing it is to be constantly assaulted by people who hate you for thinking your thoughts. Geek culture in general is fantastically vitriolic: even an issue that seems pretty marginal to the rest of us – like the question of who might play Captain America's love interest – can easily spiral into death threats. In the world of cryptography, this has been a bar to invention and progress: developers are hung, drawn and quartered every day on the internet and they have to be unusually robust to take it. The question of how to take bitcoin forward has been riven with opposing views, and after Satoshi disappeared there was no central authority to lead the discussion or calm the waters. By increments, the task fell to Gavin Andresen, a Princeton graduate with experience in Silicon Valley. Andresen only gradually accepted the role of lead core bitcoin developer. This is not an official designation and he appears to have got none of the thanks and all the flak, but by general consensus he is the most level-headed thinker in the bitcoin world. One insider said there was an irony in Andresen's situation that few people realised. 'The word is that Satoshi passed the torch to

Gavin before he retired in 2011,' he said. 'In fact, it was more like Satoshi threw the torch at Gavin and ran away leaving him holding it.'

From time to time during those months, I wondered what if, in some brutally postmodern way, the true identity of Satoshi could never be fully ascertained? What if Wright had every single element necessary to prove himself, but somehow couldn't? Anonymity – or at least pseudonymity – is an essential part of the cryptographic world. I had a job on my hands – as did MacGregor and Matthews, as would the core developers, as would the press – to establish the truth. Any narrative that is dependent on 'outing' such secretive people is at the mercy of their basic hatred of being controlled or being known, and Wright was a spectacular example of this.

*

Andresen had been in touch with Satoshi in the early days and would have records of their conversations. He would presumably be able to ask Wright questions that only Satoshi could answer. In December, after *Wired* published the story about Wright possibly being Satoshi, Andresen told the magazine he'd never heard of Craig Wright. But he began to believe in Wright once he started corresponding with him by email in early April. At one point, Wright sent him two emails, one written in his own Craig Wright way, and another one, with essentially the same content, written as Satoshi would have written it. They discussed maths and the history of the invention and the problems it had faced. Within a week, Andresen was sufficiently convinced to get on a plane to London. He was ready to see Wright sign a message to him using the original Satoshi cryptographic keys.

At this point, I began talking to Andresen. He told me he had written an email to Wright before getting on the plane, asking for a little more of his backstory and for his thoughts on 'the state of bitcoin in 2016'. 'He replied with a longish email,' Andresen told me, 'on the state of bitcoin and why he decided to reveal his secret now, then followed up with a couple of in-progress research papers. The email

“sounded like” the Satoshi I worked with, and the papers matched his academic, math-heavy voice, too.’

Andresen crossed the Atlantic overnight, arriving at the Covent Garden Hotel at 11 a.m. on 7 April. He went to his room – which had been booked, as had his flight, by nCrypt – and had two hours’ sleep, after which MacGregor and Matthews turned up. ‘They gave me a lot of the background and explained their involvement,’ Andresen told me. When Wright turned up at the hotel, Andresen found it easy to talk to him, ‘although I was so jet-lagged at one point,’ he wrote, ‘I had to stop him from diving deep into a mathematical proof he’d worked out related to how blocks are validated in bitcoin.’

Matthews had booked a conference room in the basement, and MacGregor could see that Wright was very emotional when he entered the room. ‘He knew this was it,’ MacGregor said to me. ‘It’s one thing to prove his identity to you and me, but the bitcoin community is something else. He knew that they would believe Gavin. He knew this was it – that he would have no plausible deniability after he’d talked to Gavin and shown him the keys.’ Before the meeting in the basement properly started, Andresen said to MacGregor – as he said to me – that some of the phrases Wright had used in their email exchange had been ‘familiar’ to him; he sounded like the Satoshi he had been in contact with before. Andresen asked MacGregor and Matthews a few questions about what nCrypt hoped to achieve with this in the future. They didn’t go into detail about the company’s business plans, but they spoke about the future of bitcoin and alternative projects. Wright and Andresen quickly started scribbling on pieces of paper. Wright was using his big laptop to show his access to certain addresses. It was a strange situation in all sorts of ways, and the main one, perhaps, was that Andresen, who had, once upon a time, left behind high-paying job opportunities to work on the bitcoin project for free, was possibly about to meet his hero. But he stuck to practical questions. He asked Wright about the trust and about his bitcoin holdings and what had happened to them. MacGregor later told me that his first question after Matthews told him that

Wright was Satoshi was: ‘Well, why isn’t he sitting on an island surrounded by piles of gold?’

Wright became quite relaxed. He explained what it had cost him to keep his companies alive and to pay for research and development, and the supercomputer. It was about 5.30 p.m. when he finally logged on to his laptop to do for Andresen what he had done for me in his office at home, sign a message with the key and have it verified. Andresen looked on. Wright had just used Satoshi’s key. At that point, it seemed to some of those in the room that Andresen’s body language had changed; he seemed slightly awed by the situation. He reached over to his bag and took out a brand-new USB stick and removed it from its wrapping. He took out his own laptop. ‘I need to test it on my computer,’ he said. He added that he was convinced, but that if people were going to ask him, he had to be able to say that he’d checked it independently. He pointed to Wright’s laptop and said it could all have been pre-loaded on there, though he knew that was unlikely. But he had to check on his own computer and then they would be done. He said the key could be used on his laptop and saved to the memory stick and that Wright could keep it. But for his own peace of mind, and for due diligence, so that there wasn’t a chance of fraud, he had to see it work on a computer that wasn’t Wright’s own.

Wright suddenly baulked. He had just signed a message to Andresen from Satoshi, he said, and had demonstrated his complete familiarity with their correspondence, but, in his mind, what Andresen was now asking for was of a different order. ‘I had vowed,’ Wright told me, ‘never to show the key publicly and never to let it go. I trusted Andresen, but I couldn’t do it.’ Wright got up from the table and started pacing. He had clearly believed he would be able to get through the proof session without this. In fact, he had said in my presence several times over the preceding months that he would never hand the key over to anyone or allow it to be copied or used on someone else’s machine. ‘I do not want to categorically prove keys across machines,’ he wrote to me in an email. To him, this would be to give Satoshi away and perhaps to dilute his own proclaimed connection to him. He went to a chair in

the corner of the room and looked up at Andresen. ‘Maybe you and I could get to know each other better,’ he said.

Andresen just nodded his assent. ‘Like, trade more emails,’ Wright said, ‘and I can sign more messages to you.’

At this point, Matthews’s blood ran cold. ‘It was the only time during all the years that I thought: “Jesus Christ, has he been spinning us the whole time?”’ MacGregor too felt this was a very risky moment. He glanced at Matthews. There was no way he was going to let Andresen get back on the plane with *that* as a punctuation mark. They all felt Wright’s behaviour was ludicrous: he’d demonstrated that he was Satoshi and only had to let this be verified on Gavin’s laptop. End of story. But Wright spoke to me later in a way that showed his old cypherpunk suspicion had reared its head: what if Gavin was a plant? What if the whole thing was a plot to rob him of Satoshi’s keys and exploit him or deny him? Wright told me he felt strong-armed and that, for some reason, he couldn’t let this thing go and remain himself.

Afterwards, Andresen was sanguine. ‘The proof session took longer than expected,’ he told me. ‘I insisted that the verification happen on a computer that I was convinced hadn’t been tampered with. And they’ – Wright, Matthews and MacGregor – ‘insisted that the signed message never touch a computer that could have been tampered with (the risk would be that the proof might leak out before the official announcement). So we waited a bit while an assistant went to a computer shop and got a brand-new laptop.’ The idea had been MacGregor’s. He said the tension in the room was unbelievably high. Wright was refusing to do the one thing that would guarantee the success of his mission. He hadn’t seen it coming, but Andresen wouldn’t blindly trust Wright’s hardware, and Wright wouldn’t blindly trust Andresen’s. The solution had to be a fresh computer straight out of the box. MacGregor called his assistant and gave her the task. ‘This is how you get your One,’ he said to her. (In his company the best score you could get in a staff appraisal was a One.) It was just before 6 p.m. on a Friday night and they needed a

brand-new laptop in Covent Garden. The assistant got hold of one and rushed over from Oxford Circus to the hotel.

The new laptop was lifted out of the box. It took a while to connect it to the hotel's wifi and to load the basic software. 'During all that time,' Andresen told me, 'it was obvious Craig was still, even then, deeply hoping his secret identity could remain secret. It was emotionally difficult for him to perform that cryptographic proof.'

'It was tense and there was a bit of shouting. There were a few drops during the day about "the evil businessman in the room",' MacGregor said. 'He stopped short of accusing Gavin of having a key-logger, but he clearly wasn't going to do it. He said he had trust issues, and he'd been attacked, and it had been so long, and he just couldn't bring himself over the line today, but they should keep talking. And Gavin was willing to do that. But we were like: "No, no, no". I remember what I said. I said, "Look, Craig, you've just been alone for way too long. Gavin has dedicated a huge chunk of his life to what you invented. I think he has the right to see this. He is the friend you don't have: Stefan and I can't fill that role for you; Ramona can't. This is someone who really understands what you have been trying to do."'

There were long silences. 'He was on the edge,' MacGregor said. Matthews was practically holding his breath. He didn't want to say too much out loud, so he texted MacGregor. The text said: 'He should call Ramona.' While MacGregor was out of the room Wright phoned his wife, and she said: 'Do it.' Everyone waited with bated breath as Wright used the new laptop to open the Satoshi wallet and set about signing a new message to Andresen. It failed. It wouldn't verify. He tried it again and again, until Andresen remembered that Wright hadn't typed 'CSW' at the end of the message the way he had in the original, the one he was seeking to verify. When he put 'CSW' at the end of his message to Gavin it said: 'Verified'. Wright had demonstrated, on a brand-new laptop, that he held Satoshi's private key. They stood up and shook hands and Gavin thanked him for all he had done. There were tears in Wright's eyes. 'His voice was breaking,' MacGregor told me. 'Gavin could see he was going though something.' Both MacGregor and Matthews later said that

Wright was turned inside out by the session. ‘I didn’t want to just put him in a taxi,’ MacGregor said. Andresen was wiped out, so he went to get some fish and chips, and then headed to bed. ‘Craig broke down,’ MacGregor told me. ‘He said he thought he’d never have to do this. He said he never knew how to trust people in his life.’ Wright and Matthews and MacGregor went off to find a bottle of wine. ‘He was semi-apologising for being a pain in the ass,’ MacGregor told me, ‘but I understood more than ever, at that point, how hard the whole thing was for him.’

When I asked Andresen if he thought ending the Satoshi mystery might be good for the technology, he wasn’t sure. ‘On one hand,’ he said, ‘having a mysterious founder is a great creation myth. People love a creation myth. Knowing the real story might make bitcoin less interesting to people. On the other hand, money is supposed to be boring – something that “just works”, used by most people without understanding how or why it works. I’m excited to see how Craig contributes to making bitcoin work even better than it does today.’ I later met with Jon Matonis, who had been through his own proof session with Wright. He was equally impressed and relieved. He too believed the search for Satoshi had come to an end and he was looking forward to working with Wright, to seeing the patents and the new blockchain ideas. During our lunch in Notting Hill, Matonis suggested that this technology would change the world. One of the scientists said to me, ‘This isn’t Bitcoin 2.0. This is something magnificent that will change who we are. This is Life 2.0,’ and Matonis agreed.

The idea was now to use the ‘proofs’ – the gathered papers, the testimonies of the two bitcoin experts, the use of the keys, plus solid, document-heavy answers to every criticism previously made of Wright – and roll them out to selected members of the press on a certain day. I told MacGregor and Matthews I didn’t want to go first with the story. I wanted to sit in on the interviews and proof sessions with the media organisations, and fold their reports, and the response to their reports, into my story.

Wright began to fade as we entered the proof sessions. He went from being a man with a clear picture of himself, to being a fuzzy screen. He would email me at all

hours with a pressing sense of anxiety. He seemed to be losing it. Yet we all forged ahead to a conclusion that seemed much more conclusive to him than anything he had ever expected, or could ever bear. He had signed up for it and was now faced with a full-frontal assault of cameras and lights. I had once asked him if he felt happy hiding in the internet and he said yes, it was his home. On a good day it is the bright field that contains all souls but on a bad day it is the final darkness, where misery is gapingly exposed. I came to believe that Wright, this last year, was fighting for his soul on that plain, like Aeneas with his ships at his back and all hell in front of him, going down to an underworld where he might meet his own father. Wright told me, without demur, that his life had been an attempt to prove himself to his father. In the wee small hours, he seemed like a child whose fantasy had gone too far. And the fantasy was not that he is Satoshi. He may well be Satoshi. The fantasy was that he could live as Satoshi, and take his place among the great men, and forget the little boy who was slapped for losing at chess. Like Aeneas, he knew that his journey was as much ordeal as opportunity, and though, again like Aeneas, he had asked for it, the process was increasingly unendurable. ‘It is easy to descend into Avernus,’ the Sibyl in Seamus Heaney’s translation of Book VI of the *Aeneid* tells Aeneas:

> Death’s dark door stands open day and night.
>
> But to retrace your steps and get back to upper air,
>
> That is the task, that is the undertaking.
>
> Only a few have prevailed, sons of gods
>
> Whom Jupiter favoured, or heroes exalted to glory
>
> By their own worth.

**The Reveal**

By my last weeks with Craig Wright, I was in two minds about the money men, probably because I liked them. And while I wanted to assert my journalistic doubts – preserve my innocence, stand back from the parade – my wish for the reveal to turn out well was beginning to cajole my judgment. I was wise enough to say no to the world exclusive; I still wanted material I didn't have and I was convinced that the real proof of the pudding would be in the world's tasting of it. The internet is great at crowdsourcing facts and establishing the accuracy of stories, and I had always felt this could be important. But in the meantime, I had to fight to give my doubts the oxygen they needed. The nCrypt boys said they understood – but did they? They appeared to have no Plan B if Wright couldn't prove to the world that he was who he said he was. People can start off by saying, 'Write everything, warts and all,' and end by saying: 'I don't exist, maybe you shouldn't mention me.' In a conversation with MacGregor at this point, I allowed for the possibility that I might give him a made-up name in the story. I said it because he seemed anxious, and because, as I told him at the time, he had brought the story to me and I meant him no harm – but this possibility depended on its being proved that Wright was Satoshi. Our discussion about using real names was inconclusive – during a later meeting at Berners Tavern, Matthews expressed the view that I should put their names in and make a final decision later – but the decision was really made by what the story became. The men in black seemed not to have prepared for any of that. They believed that only one big thing was going to happen: Craig Wright was going to emerge as Satoshi Nakamoto, the great mystery figure of the digital age, and the evidence would be 'overwhelming'. In the final week, as the men prepared the reveal, I found my independence slipping. No doubt about it: I felt like part of the team. I wanted to please MacGregor – pleasing people is my chief vice as a man and my main virtue as a reporter – but I could have told him my work so far might only be fieldwork. I wouldn't know how the story would turn out until it had turned out. Only in public relations is the story straight in advance.

In private, Wright was still saying he wouldn't 'jump through hoops', but then I'd find him agreeing to do exactly what was asked of him. Only a few nights before the

media appointments, I was sitting with him in the Coach & Horses in Greek Street. The PR company, he told me, had asked if he wanted to go on TV, and he'd said there was no way in hell they'd get him in front of a TV camera. Yet it was all happening. I mentioned the fact that MacGregor, when I first met him, had spoken about all this ending with a TED talk in which Satoshi would be revealed.

'Rob always said "eventually",' Wright replied.

'But what does "eventually" mean?' I asked.

'It originally meant, "*if* you came out",' Craig said.

The PR team, at MacGregor's behest, had been in touch with a number of journalists; the ones who were interested were from the BBC, the *Economist* and *GQ*. The inclusion of *GQ* had irked Wright from the start (he sees himself as an academic), but the PR company, the Outside Organisation, had a connection there – their founder was a contributing editor – and said the magazine would love the story. But did the PR men explain to the editors there who was behind this project to out Satoshi, and who was paying their fee? I later asked them by email and one of them replied: 'It is not at all unusual to be instructed to represent an individual through an independent company. Our conversation with [*GQ*] and the other journalists was about the proposed story.'

I emailed him again. 'But did you tell them,' I wrote, 'that the outing of Satoshi was being done at the behest of a commercial company?' He didn't reply.

All the journalists had signed NDAs and embargos. They would each be allowed a brief interview with Wright after he had demonstrated to them his use of the Satoshi key. These meetings would take place at the offices of the PR company in Tottenham Court Road on Monday, 24 April and Tuesday, 25 April. I found all this a bit odd: Wright was being difficult, for sure, but the PR strategy was crazily old-fashioned. Everyone in the cryptography world knew that all Wright had to do was send an email from the famous Satoshi email address, alert people he was

going to sign a message using Satoshi's keys, do so online and move a single bitcoin from an early block, and the entire internet would light up like Coney Island for the World's Fair. The piecemeal feeding of 'proof' to these journalists was compelling but anachronistic. I supposed it was an attempt to get the story out of the world of crypto-gab and into the real media, but it was set up with an alarming sense of security paranoia. Wright could never have handled a celebration, but the journalists were being managed to an extent that might have raised more questions than it answered. I was just an observer, and was worried about Wright by then, and, though I believed in him, I felt distinctly that there was something missing and something wrong.

When I turned up at Starbucks in Tottenham Court Road, Wright, Ramona and Matthews were already there. Wright was sulking a little. It had been decided that, as well as the demonstration, the journalists would be given a memory stick to take away with them, showing the signed Satoshi message. (Wright later told me the stuff he put on it was fake. There wasn't anything on there they could understand, but it certainly bore no relation to any of Satoshi's keys.) Matthews was dressed smartly and wearing dark glasses and Wright was wearing a gold tie and a business suit. Ramona sat beside him stroking his ear. 'Let me know if you have trouble with the guys upstairs,' Matthews said. He meant the PR guys. 'Sometimes they forget their role.' As usual, I found Matthews likeable and easy to talk to, but he seemed not to appreciate the difference between his way of talking and the circus of manipulation surrounding us.

Rory Cellan-Jones, the BBC's technology correspondent, was led into a conference room with his producer, Priya Patel, and Mark Ward, a technology correspondent for the BBC News website. Wright sat at his laptop, hardly looking up, and a screen on the wall showed what he was looking at. Matonis was in the room, and so was Matthews. Ramona had gone upstairs. Cellan-Jones was decent and professional, ready to get to the bottom of the story. He appeared to feel the tension, with Wright already behaving as if being asked questions was grossly humiliating and the

questioner openly hostile. But Cellan-Jones was not hostile: if anything, he was mildly pre-convinced, and just going about capturing the story for the layman.

‘When I started out I asked myself what I’d need to see to know if someone who claimed to be Satoshi was Satoshi,’ Matonis said. ‘And you can break down three distinct lines of evidence: the cryptographic line, the social line and the technical line. Obviously, the social and technical lines are going to be more subjective … On the cryptographic side, I’ll explain what I witnessed personally and give you a lead up to what Craig’s going to demonstrate this morning.’

He then went into more detail about the cryptographic proof. ‘The Genesis block is block zero,’ Matonis said. ‘And you can’t spend any of the blocks in that chain – which means that the ones that come after that (which are spendable) can be attributed to the creator of bitcoin.’

‘And what would they be called?’ Cellan-Jones asked.

‘In succession they’d be called block 1, block 2 etc. Now this morning, Craig is going to demonstrate signing blocks 1 through 9. I personally witnessed the signing of blocks 1 and 9, so this is not going to be a transfer of bitcoins, it’s going to involve a signing of a message, which he’ll do with the private key and which will be verified by the public key. Are we clear on that?’

Eventually, Wright asked Cellan-Jones to give him a message. ‘Um. “Hi, historic message to the BBC.”’ Wright typed the message and added a bit of commentary as he did so.

‘This message will verify, but if I change a single digit, it won’t,’ Wright said as he signed the message using block 9.

‘This is the only key that we know is definitely owned by Satoshi because it was used with Hal Finney,’ Matonis added.

‘So,’ Cellan-Jones said, ‘just getting this clear in my mind. We’ve seen Craig use a private key known to have been used with Hal Finney. And we’ve seen it verified with the public key.’

‘Yes,’ Craig said. Then he proceeded to sign a message with the key associated with the first ever mined bitcoin.

‘Out of interest,’ Cellan-Jones said. ‘How many bitcoins do you have?’

‘Well, that would be telling,’ Wright said.

‘Do you still mine bitcoins?’

‘Only for fun.’

Wright then went into an aria about Sartre’s speech when he turned down the Nobel Prize. He planned to use a hash function – which turns information into a unique set of letters and numbers – to attach Sartre’s famous speech cryptographically to block 9, and then later verify it publicly on his blog. ‘He gave up the prize,’ Wright said, ‘because “If I were to accept it, I’d become the institution.” I never wanted to sign Craig Wright as Satoshi,’ he continued. ‘I haven’t done this because it’s what I wanted, I just can’t refuse it. Because I’ve got staff, I’ve got family. It’s what I am and I’m not going to deny it because that’s not the truth. So I’m choosing to sign Sartre because it’s not my choice, I’m not choosing to come out, I’ve been thrust into it.’

‘In what way have you been forced into it?’ Cellan-Jones asked, quite reasonably.

‘I’ve got people mudslinging,’ Wright said. But that wasn’t true: he wasn’t feeling forced because of what people said. He felt forced, or obliged, to come out because he’d signed the deal with nCrypt in June 2015. And he deepened the lie when Cellan-Jones asked him why he hadn’t revealed himself before. ‘I liked to go to

conferences, put out papers,' he said. 'I can't do that now. I can never just be Craig again.'

He was asked whether he wanted to be the public face of bitcoin.

'I don't want to be the public face of anything.' He paused and looked down. He then said that his blog would explain everything and help people to download the material and understand how the keys work.

'When does that go live?' Cellan-Jones asked.

'Monday or Tuesday.'

'There will be people out there who will try desperately to prove this isn't the case. Are you confident that there are no chinks in your armour?'

'They'll say I stole keys, that I buried Satoshi in a ditch, they'll say all sorts of things.'

The BBC planned to come back the next day with cameras. Then a man arrived from the *Economist*, Ludwig Siegele, a man in a grey suit. He was less immediately friendly but his questions were fine-grained. You could see he wasn't entirely comfortable with this very PR-managed way of outing Satoshi. Wright signed a message for Siegele using block 9, and had the private key verified by the computer. 'I'm sorry,' Siegele said, 'but I'm still a little unsure what that proves.'

'It proves I have the private keys,' Wright said. 'All the original private keys.'

'OK, so. The first question that my readers are going to ask is: "Why now?"'

Wright didn't hesitate. He was using his media training. 'I've tried to avoid media,' he said, 'but it's starting to affect other people. I'd prefer to stay quiet. Why now? I have staff, I have family … All the innuendo, the falsehoods.' He had never suggested to me, in all our months of interviews, that he was outing himself because of media misrepresentation. I accepted it, though, when he said it to these journalists,

imagining that perhaps he had realised that the tax office pressure was the real pressure in his life, the thing that forced the outing. I said this later to the nCrypt guys and they agreed.

‘Why conceal your identity anyway?’ Siegele asked.

‘I don’t want to be a public figure,’ Wright said. ‘I hope people don’t listen to Craig Wright. They will look at the facts, not decide based on what Satoshi says.’

That afternoon, I went to another appointment while Wright went off to Parsons Green to have his photograph taken for *GQ*. The next morning, at Starbucks again, Matthews was ridiculing the whole business with the photographs, and making fun of the magazine’s original idea that he wear a mask in one photograph and rip it off in another. Matthews described what happened at the interview with the magazine’s senior commissioning editor, Stuart McGurk. ‘It actually went quite well,’ Wright told me. ‘The journalist was nice, but he brought along this complete wanker of an “expert”.’

The man they were talking about is a university lecturer in cryptology. McGurk brought him along to help verify the claims. ‘It was hilarious,’ Matthews said. ‘Craig threw the guy out.’ According to one witness, he’d questioned Wright quite forcefully about his understanding of public and private encryption keys. ‘He was totally in the guy’s face at one point.’

‘He was telling me he was more qualified than I am,’ Wright said. ‘It became a nice interview but this guy was a complete idiot and I told him to get the fuck out.’ Matonis – who was there – said the scene was intense. I wasn’t sure it was wise to greet dissenters and opponents, even ones who might be wrong, that way, but Wright was roundly applauded for doing so. I confess I felt it was wrong to tell journalists only half of the story, allowing them to misunderstand the reason he was suddenly coming out as Satoshi.

*

That day, the BBC came back. Wright was more irate than he had been the day before and less co-operative now that the camera crew was here. He felt he had done much more than he had ever wanted to and he said so, mainly under his breath. The cameraman set up the camera and then Cellan-Jones got into position. ‘So who are you? And what are you about to show me?’ he asked.

‘My name’s Craig Wright, and I’m about to demonstrate the signing of the message with a key that is associated with the first transaction ever done on bitcoin – a transaction of ten bitcoin to Hal Finney.’

‘And who did that first transaction?’

‘I did.’

‘And whose name is associated with that transaction?’

‘The moniker is Satoshi Nakamoto.’

‘So you’re going to show me that Satoshi Nakamoto is you?’ Craig looked bewildered for a second and hesitated.

‘Yes,’ he said.

‘Are you confident that this will prove to the world that you are Satoshi?’

‘It proves I have keys … other things we’ll be releasing will help … Some people will believe and some people won’t, and, to tell you the truth, I don’t really care.’

‘But you can say, hand on heart, I am Satoshi Nakamoto?’

‘I was the main part of it. Other people helped. At the end of the day, none of this would have happened without Dave Kleiman, without Hal Finney, and without those who took over – like Gavin and Mike.’

‘And this is going to have a huge effect on your life?’

‘Unfortunately, yes.’

Something changed in Wright in those few minutes. With these direct questions about Satoshi, his sense of himself – I don’t know how else to put it – had come unstuck and he became noticeably uncomfortable. He said that he wanted to make the point that people should stop looking to him for answers.

‘Make that point upstairs,’ Cellan-Jones said.

‘Upstairs?’

‘We’re going to film a straightforward interview upstairs, without the computer.’

Wright muttered something and stared into the depths of his computer as if he wanted to escape into it and never come out. ‘I just want the basis to be on the computer,’ he said.

The female producer interjected. ‘Because we haven’t actually done that bit on camera yet,’ she said.

The PR executive came over, a little red in the face. ‘Can we do that bit upstairs?’ he asked. ‘Are we all right to do the “why now?” question upstairs? And we’ll be done?’

‘You know, I don’t actually watch TV,’ Wright said.

The BBC left the room to scout out the location for the proper ‘sit-down’ interview. Wright complained to me that he was being pushed. ‘I just didn’t want a big facial

shot of me,' he said to the PR man. 'I preferred to be behind the screen a little bit … I'm not against it, as long as I can hide behind the screen.' The PR man said he didn't have to do anything he didn't want.

'I'm just doing the one question,' Wright said. The PR man left the room leaving me alone with him.

'Does it feel completely against the grain of your nature to be asked, "Are you Satoshi?" like that?'

'Yes.'

'Is it a crude question to you?'

'Why does it matter, other than that you need someone to attack, someone to deify. I mean, fuck's sake. I'll do this. That's it. Fuck off. I can dance around saying "please believe me." But it's more than absurd, it's melting clocks on a landscape.' At that point, the door opened and the PR consultant came in.

'Craig,' he said, 'we've explained to the BBC that you want to stay down here, and they're all making the point that this is the last thing you'll ever do …'

Craig started shaking and pushed his chair back. 'No! No! No!' His face was pale. 'You see this door,' he said. 'I don't want to hear another word. It's here, it's my way.' Then he walked out and slammed the door, leaving me alone in the room with the PR boss.

'We're only doing our job,' the boss said, with a shrug. Wright came back a second later and his microphone pack was trailing behind him.

'It's my way or I don't come back. OK? I'm not doing this for fucking PR stuff, I'm not doing this for anyone else. I don't give a fucking shit about what people say, I'd rather not do it. One word about it and I'll never come back. Not exaggeration. I will

never enter this office again. I'll never answer an email again, and I'll never talk to another PR person in my life again … Got it?'

'Yeah,' the boss said.

'Thank you.'

He went out and I was alone with Wright again. 'They've already pushed me,' he said. 'I'm already beyond where I want to be: I'm already doing a TV thing. And everything is always: "Let's take it a little bit further, a little bit further." Which bit of "Go away" don't they get?'

I asked him if Kleiman would have handled it better. 'Better than I do,' he said. 'He would still have told them to fuck off. But in a nicer way. Hal would have done it far better.'

'What do you think they're talking about up there?' I asked.

'The fact that I don't want to jump through their fucking bloody crap. "This man has a big credibility gap he's got to overcome, I'm open to being convinced he's Satoshi but …"'

The BBC came back downstairs to ask their 'one question' and, naturally, Cellan-Jones asked more than one. In the panicked and hostile mood Wright was in, he needed scapegoats, and the PR weren't meat enough and Matthews was too much the boss. So he scapegoated the BBC, saying, as soon as they left the room, that they had broken their 'contract' with him, that they were liars. 'I'll never do any television interviews again in my life,' he said. 'Never.' And as he said it, I was imagining him with Fox News or the rottweiler interviewers. 'The whole thing was just an attempt to expose me as being something I'm not,' he said.

'That was actually a pretty softball interview, Craig,' I said. 'You can't blame them for turning up and asking for proof.'

'Are you talking about proof or evidence? You're conflating the two. They're not the same and that's one of the things I'm saying. I gave them proof. They want more.'

Wright was happy to lecture you day and night about algorithms, but he wouldn't name names, and he struggled to provide real-world evidence of Satoshi's footprints. The more I thought about it, the more I realised something was wrong, for him, with the footprints analogy, because if Satoshi was only one man he would only have one set of prints. The Satoshi who existed online could be any number of people. But there was something revealing about his treatment of the BBC – something not very nice in his attitude to people who make it their business to ask straight questions – and the handling of the proof sessions made it clear how much of a danger he was to his own credibility. A month later, when I asked Cellan-Jones if the PR company had ever explained to him that there was a commercial company behind the outing of Satoshi, he said he had never been given that information, 'just that they were representing the man who was Satoshi'.

**Life Rights**

At 7.51 A.M. on 2 May 2016 all was quiet on the Twitter front. Well, not quiet, but the names Satoshi Nakamoto and Craig Wright were nowhere to be seen. This was the day of reckoning, the day the embargo would lift and the media outlets could run their pieces and name Satoshi. At 7.55, *Game of Thrones* was trending and so was Gerry Adams, for allegedly using the word 'nigger'. Also trending was a wildfire in Fort McMurray and a bombing in West Bengal. There's a strange feeling of supreme calm before a storm breaks. At 8 a.m., Wright posted a blog containing the supposed hash of the Sartre speech and various postings about himself as Satoshi. At the same moment, Gavin Andresen posted a message to his blog. Title: 'Satoshi'. 'I believe Craig Steven Wright is the person who invented bitcoin,' it began.

> I was flown to London to meet Dr Wright a couple of weeks ago, after an initial email conversation convinced me that there was a very good chance he was the same person

I'd communicated with in 2010 and early 2011. After spending time with him I am convinced beyond a reasonable doubt: Craig Wright is Satoshi.

Part of that time was spent on a careful cryptographic verification of messages signed with keys that only Satoshi should possess. But even before I witnessed the keys signed and then verified on a clean computer that could not have been tampered with, I was reasonably certain I was sitting next to the father of bitcoin.

During our meeting, I saw the brilliant, opinionated, focused, generous – and privacy-seeking – person that matches the Satoshi I worked with six years ago. And he cleared up a lot of mysteries, including why he disappeared when he did and what he's been busy with since 2011. But I'm going to respect Dr Wright's privacy, and let him decide how much of that story he shares with the world.

We love to create heroes – but also seem to love hating them if they don't live up to some unattainable ideal. It would be better if Satoshi Nakamoto was the codename for an NSA project, or an artificial intelligence sent from the future to advance our primitive money. He is not, he is an imperfect human being just like the rest of us. I hope he manages to mostly ignore the storm that his announcement will create, and keep doing what he loves – learning and research and innovating.

I am very happy to be able to say I shook his hand and thanked him for giving bitcoin to the world.

Also at 8 a.m., with the embargo lifted, the first tweet appeared, from Rory Cellan-Jones: 'Craig Wright tells BBC I am bitcoin inventor Satoshi Nakamoto, publishes evidence backing his claim.' One minute later, a tweet appeared from @CalvinAyre, naming Craig Wright as the proven Satoshi. The *Economist*went one minute later, with a link to Ludwig Seigele's open-minded piece asking for more and better evidence. At 8.09 a.m. Radio 4's *Today* programme broadcast Cellan-Jones's report. 'I'm about to demonstrate the signing of a message with a key that is associated with the first transaction ever done on bitcoin.' The report was brief and quoted Wright once. It said Wright hoped to disappear and that that would be

difficult. They played the part of the interview where Wright said he was part of the group behind Satoshi.

‘He sounds plausible,’ Justin Webb, the presenter, said, laughing. Then they played part of the interview with Matonis, who said he was ‘100 per cent convinced’.

‘Why should people be excited by this?’

‘I put it on the level of the Gutenberg printing press,’ Matonis said.

‘Quite a lot of people are saying that this is as important as the internet,’ Cellan-Jones reported, ‘and that this man – if he is the man – should be celebrated like Tim Berners-Lee.’

‘Craig Wright has just outed himself as the leader of the Satoshi Nakamoto team,’ the bitcoin insider Ian Grigg wrote on his blog:

> Sometime in summer of 2015 the secret started to spread, and the writing was on the wall. An extortionist and a hacker started attacking, perhaps together, perhaps apart; to add to the woes, Dr Wright and his companies were engaged in a long harsh bitter battle with the Australian Tax Office. Since then, the team has been more or less in hiding, guarded, at great expense and at some fear … Satoshi Nakamoto dies with this moment. Satoshi was more than a name, it was a concept, a secret, a team, a vision. Now Satoshi lives on in a new form – changed. Much of the secret is gone, but the vision is still there. Satoshi Nakamoto is dead, long live Satoshi. Yet, a warning to all. Satoshi was a vision, but Craig is a man. The two are not equal, not equivalent, not even close … It is true that Craig is the larger part of the genius behind the team, but he could not have done it alone.

Over the following two hours the words ‘Craig Wright’ were typed into search engines tens of thousands of times, and the Reddit forums and the cryptocurrency community got to work. Meanwhile, I was being copied into the emails sent from the PR company to nCrypt and the Wrights. It issued a press release spreading the news to less favoured outlets. ‘Wright’s decision to go public follows a series of

misleading statements that are circulating and which he seeks to set straight,' the release said. 'Wright has also launched a blog, with a vision to create a forum about bitcoin, which dispels myths and helps to unleash its full potential. He will create a space to provide developers and producers with the real facts about the technology so as to encourage the widespread use of bitcoin and the blockchain.'

'Great start!' the top PR man wrote to the group at 9.31 a.m.

'Ta. All going well,' Wright wrote just before ten.

'All going to plan,' the second PR man echoed a few minutes later.

'Right on course so far,' the first PR man wrote at 10.13 a.m. And that was the last of the good news to come from the world of public relations.

By midday the blog was receiving the wrong sort of attention. A number of researchers had studied what Wright had written and noticed that the explanation was fudged – worse than fudged, it was faked. Something that he said was signed with the Satoshi key had, in fact, been cut and pasted from an old, publicly available signature associated with Nakamoto. It was astonishing and the buzz quickly grew fierce. All those hours in secret flats scrolled through my head. There had always been something missing, something he hadn't wanted to show. But was that because he wouldn't, or because he couldn't? The thought that he would fake proof so publicly and so coarsely was hard to comprehend. He sent me an email. 'They changed my blog post,' he wrote. 'It will be back as I wanted. But first I need to negotiate with Stefan.' And I replied: 'How did they change it?'

I thought he was lying. He had lied before, but to lie so transparently and so publicly made me think he had lost his mind. There was no way to square such actions with his wish to have no publicity. He had faked his own proof, and now he was being ripped apart on the internet. I briefly wondered if he might be enjoying the cries of execration, but how could he do that to Andresen and Matonis? Suddenly his opponents seemed wiser and greater in number. It took me a few days to see that

Wright's action might be consistent with something deeper in his character. He never wanted to come out and when it came to it he flunked his own paternity test. But I had a feeling that that he was too close to the invention to be a simple hoaxer.

'I will explain why I think he's probably not Satoshi,' said Vitalik Buterin, a big wheel in the cryptocurrency scene, speaking at Consensus, a bitcoin conference in New York that day. A friend of mine was there. He said that men had started the day high-fiving and shouting 'Satoshi, baby', but that as the long day closed, his name became the punchline of every joke. Core developers and others were calling for him to sign something new and in public right away, using the Genesis block, which is unquestionably Nakamoto's. One of them, Peter Todd, was quoted by *Forbes*: 'All Wright needs to do, says Todd, is to provide a signature on the message "Craig Wright is Satoshi Nakamoto" signed by a key known to be Satoshi's. "This is *really* easy to do … if you're actually Satoshi. Also, you'll know sufficient proof has been provided when it actually happens, because cryptographers will be convinced."'

That was the strangest element of all: Wright must have known, having been a cryptographer all his adult life, that his fraud would be spotted immediately. But when I asked him about it he said it wasn't a fraud, it was a mistake. 'I cut and pasted something just for the time being but knew I would change it later,' he said. 'But then it went up.' That rang hollow to me, the words of a falling man. He intentionally faked it. I believed at that point that he had misled his colleagues and tried to get out of being Satoshi, which isn't necessarily the same thing as not being him. 'I can't think of a more convoluted way to go about claiming one is Satoshi than what Craig Wright has done so far,' Jerry Brito, the executive director of Coin Center, told the *Daily Beast*. 'He's provided no cryptographic evidence verifiable by the public, and many of his answers sound plain fishy.' Emin Gün Sirer, a Cornell professor who had criticised Wright before, referred to Wright's 'meta-modernist play'.

The next day, I turned up at MacGregor's office and found him sitting with Matthews in a dark meeting room. They were hunched over the desk, exhausted and

shellshocked. When I asked them what happened MacGregor shook his head. It was the first time in six months I'd heard him sounding incoherent. 'Craig happened,' he said. 'He got cute with the math. He has been trying to get consent from the trustees to get the private keys … But he wasn't allowed access to coin or to do anything other than that. So what he was trying to do was re-sign a message …' Matthews butted in, saying Wright never had authorisation from the trust to use the key publicly or let anyone take it away.

'Why didn't he just say that?' I asked.

'You tell me,' Matthews said. MacGregor went on to explain how a signed message can be used nefariously by people with enough computing power. He said the trustees didn't want anyone analysing those blocks. I'm not sure if he was grasping at straws, but what he said didn't explain the suddenness or the fraudulence of what Wright had done. MacGregor said that he and Matthews had since been with Wright and indicated that the encounter had been shouty and ugly. But he said it was OK now. 'We have verbal consent from the trustees to move coin, and we're just waiting on the written consent.'

MacGregor and Matthews had been in the meeting room for hours trying to work everything out. They thought it could all still be kept on track. MacGregor was writing new blog posts for Wright. He asked for my help with one of them and I explained that I had now to distance myself from the whole thing. I had got too close. MacGregor said they were going to 'flood the blog with evidence' and get Wright to 'move' some of the Satoshi bitcoin, to transfer it to someone else in a way that only someone in possession of Satoshi's private keys could do. Andresen had agreed to be on the other end of the coin transaction.

'Craig is being mauled out there,' I said.

Rob removed his glasses. 'The first meeting we had with him yesterday ended with: "You're fired. Buy a ticket to Sydney. You fucked us. Good luck with the ATO."'

‘He didn’t sleep last night,’ Matthews said. ‘He looks fucking terrible.’

‘He risks destroying his entire reputation.’

‘His and ours,’ MacGregor said. ‘I’ve been taking meetings with investment bankers for the last two months. I’ve pulled every string I know to get meetings with Google and Uber. If he goes down in flames, I’ll go down with him. I mean, he’s fucked me. Millions of dollars out of my pocket, nine months out of my life. But what we have now is a very pliant Craig Wright. We’re going to drag this back from the brink.’

‘It’s a big task, Rob,’ I said.

‘We finally beat him to a pulp today. No more decisions. This is what we’re going to do, because he knew the next move was pack your toothbrush and get on a plane and good luck in Australia.’ MacGregor told me he’d started Monday morning on an unbelievable high. ‘I can’t believe we kept all the puppies in the box this whole time,’ he’d thought to himself. ‘Nobody broke embargo, holy shit this is going to work. And then … ’

We spoke about Wright’s possible lies. I said that all through these proof sessions, he’d acted this like this was the last thing he ever wanted.

‘That’s not true,’ MacGregor said. ‘He freaking loves it. Why was I so certain he’d do that BBC interview the next day? It’s adoration. He wants this more than we want this, but he wants to come out of this looking like he got dragged into it.’ He told me if everything had gone to plan, the groundwork was laid for selling the patents. It was a really big deal. He said Ramona had said that if Wright doesn’t come out you still have this really smart guy who has made all these patents, who knows all about bitcoin. ‘Yeah,’ MacGregor said. ‘You and five hundred other guys who have called today.’ I shook their hands and wished them luck, thinking I would probably never see the men in black again. And as I descended in the lift, I thought I would miss their brio and their belief, despite everything.

Craig was lost in some labyrinth of his own making, or mostly of his own making. He didn't want to be Satoshi. And he didn't want to be Craig. And he didn't want to be a letdown. And yet the message boards lit up and the walls closed in. Over the next 24 hours, he agreed to move Satoshi's coin and his blog advertised the fact. It said, 'Extraordinary claims require extraordinary proof,' and he was set to provide it.

The next day, Wednesday, 4 May, Matthews was at Wright's house organising the movement of coin. The new (and final) proof session was intended to blow away the doubts created by the first. Many commentators felt it was too late, that Wright was beyond the pale, but Matthews and MacGregor had agreed with Andresen that the movement of coin, to Andresen and also to Cellan-Jones at the BBC, would undo the damage. Wright spoke to Andresen on the phone from his house – Andresen was in New York – and told him he was worried about a security flaw in the early blockchain, a problem in the way those first blocks were constructed that would make it dangerous for him to move coin, exposing him to exploitation or theft. My sources say that Andresen understood the problem and confirmed that it was all right, it had been fixed. But Wright continued to worry and was showing great reluctance about offering the final proof. Then he left the room abruptly and didn't come back.

The next day, he sent me an email. It linked to an article headlined 'UK Law Enforcement Sources Hint at Impending Craig Wright Arrest'. The article suggested that the father of bitcoin might be liable, under the Terrorism Act, for the actions of people who used bitcoin to buy weapons. Under the link, Wright had written an explanation: 'I walk from 1 billion or I go to jail. I never wanted to be out, but if I prove it, they destroy me and my family. I am the source of terrorist funds as bitcoin creator or I am a fraud to the world. At least a fraud is able to see his family. There is nothing I can do.'

He was devastated. He was the runner who failed twenty yards short of the finishing tape, the man who froze at the moment of truth, and started walking backwards. He said he feared prosecution on the one hand and humiliation on the other. The

borstal boy in Alan Sillitoe's 'The Loneliness of the Long Distance Runner' comes from a family who make much of running, 'especially running away from the police'. He hates being understood, feels authority is only there to grind you down, and holds on to his essential privacy, knowing 'they can't make an X-ray of our guts to find out what we're telling ourselves.' The boy lives on his own terms, which means not faking it for power, even when the pressure is high and the rewards are obvious. So he refuses to win. Representing the borstal in a championship race he is well ahead of the other runners, but he stops, and lets them pass, and at the end jogs up to the tape: 'I got to the rope,' Sillitoe writes, 'and collapsed, with a murderous-sounding roar going up through my ears while I was still on the wrong side of it.' In another email that day Wright wrote: 'Andrew, I don't know what I can say. If I was to do the proof and save myself, I damn myself.' That afternoon, he closed down the blog – the one that was intended to lead cryptocurrency fans into a new era – but left a final posting:

> I'm sorry. I believed that I could do this. I believed that I could put the years of anonymity and hiding behind me. But, as the events of this week unfolded and I prepared to publish the proof of access to the earliest keys, I broke. I do not have the courage. I cannot. When the rumours began, my qualifications and character were attacked. When those allegations were proven false, new allegations have already begun. I know now that I am not strong enough for this. I know that this weakness will cause great damage to those that have supported me, and particularly to Jon Matonis and Gavin Andresen. I can only hope that their honour and credibility is not irreparably tainted by my actions. They were not deceived, but I know that the world will never believe that now. I can only say I'm sorry.
>
> And goodbye.

*

The next morning I drove through the traffic to a London suburb. It was early in the day and the high streets were empty, the happy boutiques, the delis and the wicker-and-candle dens where people come to improve their mood or do something

about their lifestyle. Craig and Ramona were sitting in the corner of a popular café. They were holding hands and staring at the table. He was wearing his Billabong T-shirt – I remembered it from his description of the clothes he'd bought in Auckland when he began his long-distance run last December. He looked as he'd looked the first night I met him in Mayfair: unshaven, unslept, the scar on his face more livid, his pupils like pinpricks and his breathing heavy. He wasn't just white, he was empty-looking, and his hands were trembling. Ramona was crying. The light of the café seemed too much for the darkness enclosing them. I went to shake his hand but we hugged instead, and it was like embracing a drowning man. He hadn't really slept since Monday and this was Friday. He wasn't drinking his latte, he made clouds on the spoon, and stared.

'Well, it was worth about a billion dollars to them,' he said. Ramona talked about jail and I asked if they were afraid of being prosecuted.

'They say it'll never happen,' she said. 'Of course it will … So how can he? How can he?' He spoke of men he knew who had sold bitcoin and had been prosecuted for money-laundering and said they might try to do that to him. 'It was always a present danger,' Ramona said. MacGregor, Wright alleged, had always had a plan to move him if necessary to Manila or Antigua if it looked like he might be arrested.

'It's always been incremental,' Craig said. 'One step, one step, and nobody realises that eventually that takes you over a precipice.'

'That's the thing,' Ramona said. 'Your happiness doesn't count at all. But now we're stuck. You come out – you go to jail. You don't come out – you're a fraud. It's got to the point where it's almost better if he's a fraud.'

'So what happened on Monday,' I asked, 'when it came to writing that blog?'

'I gave them the wrong thing,' he said. 'Then they changed it. Then I didn't correct it because I was so angry. Which was stupid. I put up the wrong one. No one wants

SN. I will never be SN. I'm not personable. You can lock me in a room and I'll write papers, I'll never be personable.'

Ramona was crying. 'They could take us down,' she said. 'They could really take you down if they want to.'

They spoke about moneymaking ventures Wright was involved in a long time ago. Wright alleged Matthews knew about these activities, which was true, because Matthews had mentioned them to me.

'I just couldn't do things anymore,' he said. 'That's all.'

They wanted to talk about the trust, but they didn't really explain it. He said it was to hide the bitcoin. 'It's not meant to be spent,' he said. 'Too many problems.'

'It's also a guarantee that you can't flood the market,' Ramona said. 'That we can't use it to pay the bills, no matter how desperate things get.' When I asked who the trustees were they went quiet.

Ramona began to worry about my story. She tried to strong-arm me. She began to tell me what I should say and what I shouldn't say and how I should hide from MacGregor and Matthews the comments she and Wright had made about them. 'I want to write the truth,' I said.

She said I knew too much. She said that Craig would go to jail or harm himself if I told everything I knew. I was stunned. There were many things that were said to me by every party in this story that I would choose not to print. Not only things they said about one another, but business arrangements and unsubstantiated allegations about the past, and things I knew in the present. But I had been recording this as a documentary from the start, as I'd said I would when we met at Claridge's in December. Now I was being told that my material was too hot and my story posed a threat.

Craig suddenly got very upset. His face crumpled and he put his head in his hands. 'And the Brits have their equivalent of Guantánamo Bay as well,' he said. 'I'll never write, I'll never see anyone. I'll be in a little room. I won't even have a pen and paper. I won't see my wife again. I'll never see …' He sobbed and was inconsolable. 'I'll never write again.'

'They won't do that,' Ramona said. I suggested they might get a lawyer to advise them on the possible threats they faced. Ramona said it was too expensive. She said the bills would run into the millions. Craig talked about Ian Grigg and others who'd 'outed' him last year by nominating him for various awards. Satoshi was nominated for a Nobel Prize and a Turing Prize. Wright told me that people in the bitcoin community wanted him to come out and receive recognition. He said it had never been in his interest to come out, but in other people's interest. 'I don't care if people like my work,' he said. 'I just have to *do* my work. That's the only thing that'll keep me sane.'

'I would like that his reputation gets redeemed but I don't know if that's possible,' Ramona told me. 'This is what I propose, if you can do it, you do it, if you can't, it's up to you. If [you say] he didn't choose to come out … then the company gets put in the spotlight. If you say you know he is Satoshi then we're in trouble. If you say you have your doubts then he looks like a fool.'

I'm sure I looked at her disbelievingly. 'You're basically saying that every version of the truth of this story is untellable.'

'But if you say it, Andrew …'

'If you were sure that this could never be said in the end, then you should never have allowed it to happen.'

'It was one step, then one step …' Craig said, again.

‘And you let a writer into your life?’ I said.

‘Do you know how much this meant to me?’ Craig said. ‘The company. The people. To be doing that. To get all these papers out. To be in that position. It’s my idea of heaven, but the cost is hell.’

‘If we didn’t co-operate with you,’ Ramona said, ‘they’d stop …’

I reminded them that every time I’d tried to walk away from this story – like when they tried to make me sign an NDA – she’d begged me to come back. I told them that full disclosure was much less damaging than any other option. Naturally enough, that was my view.

‘No one wants to believe me,’ Craig said.

‘And I think that’s great,’ Ramona said. ‘It’s great that no one wants to believe you.’

Craig said he’d **filed all these patents** and they were all from him, ‘not just Dave’.

‘What do you mean,’ I asked. ‘“Not just Dave?”’

‘I mean I wrote those patents,’ he said. ‘It means I knew all this shit.’

‘Have you been able to talk to Matonis or Andresen?’ I asked.

‘No,’ Ramona said. ‘I don’t know if they’ll even talk to us.’

‘I think you should have some crisis management advice.’

‘From who?’

‘From a therapist.’

‘We don’t have time for that,’ she said.

I walked home with them and he slumped on a sofa, looking wan, gone. ‘His mental health is fucked,’ she said to me when he was out of the room. ‘If he goes to jail, he’ll kill himself. I can’t leave him alone.’

When he returned he seemed almost paler than before. ‘This is all because I wrote code,’ Craig said. ‘Not because I blew up something, because I wrote code.’

‘Just out of interest,’ I said. ‘If you are a fraud … How hard a fraud would it have been to perpetrate?’

‘It would be the best one in human history,’ Craig said. ‘It’d be Ronnie Biggs on steroids times a million. I invented a new form of money. Who has ever had anything to do with money that wasn’t to do with government? Who has ever really succeeded?’

‘You mean it’s a thankless task?’

‘It’s always Prometheus,’ he said.

*

This was a story in which everybody wanted their story told, then untold, then hidden, back in the vaults. It seemed like a very new story, but, in fact, it was a very old one, a story of metamorphosis, and of Prometheus unbound. Craig Wright proved cryptographically that he had Satoshi’s keys, his emails seemed to show his involvement, his science extrapolated on the technology of the blockchain, and he spent a full year engaged in a business plan to reveal it all. But, when it came to it, he behaved like a fraud, he shape-shifted and he dissolved.

I began to wonder whether Craig Wright might be a man who had never known who he was, a missing person, constantly in discussion with some inner lost boy, unable to bear the conditions which forced him to say definitively who he was. Some people, it could be said, *really* aren’t anyone, in the sense that the complications of

being themselves have wiped them out. The internet eats its own ciphers, and Wright is one of them. He might have sabotaged his own proof or simply flunked the paternity test because he isn't the right man, but his own doubts about himself are the real drama. He was sick, he was brilliant, he was manipulative – but much of what he said was true. And as I drove away that morning, it was the sickness that seemed predominant. Wright was a clever man who had gone to the very end of himself to prove who he wasn't. 'We are all Satoshi now,' became a tagline for bitcoin's early fans. And in the end we all are Satoshi, and we'll begin to accept it as paper currency starts to look stale, and our minds merge with our computers. There are new networks up ahead that will have grown from the seed Satoshi planted, and it was odd, after all my travels, to believe that the only man who wanted to opt out of being Satoshi was Craig Wright. A week after his 'proof sessions' with the BBC and others, he was in complete disgrace, his corner office at nCrypt had been emptied and his leather sofas had disappeared, removed from the building with the signed Muhammad Ali picture and the rest of his stuff. Without ceremony, the best room in the office became a conference room and his name was spoken in whispers.

My last meeting with MacGregor and Matthews was a time of conjecture and anger, devastation and apology. They felt Wright had perjured himself, and for no good reason. He had never admitted to problems with the trust, problems that would, though he hadn't admitted it, make the Satoshi reveal very difficult for him. They still believe, as do Andresen and Matonis, that he is Satoshi. To them, there is just too much evidence to accept Wright's late attempt to cloak himself in deniability. But no matter. He was now fired, they said, and the deal with Google was off. 'He put a gun to our head and pulled the trigger,' MacGregor told me. 'The world is still going to think we got fooled, but I know the facts. He has the keys.' There was a moment in our meeting when I realised this had gone all the way to the bone with MacGregor. He said he never wanted to see Wright again. 'This was supposed to be so noble,' he said, 'and it became so dark.' Matthews told me that Wright's office, his house, his job, his work visa, everything, was set to go. They had spent as much as $15 million and maybe lost a billion. MacGregor said the PR company would never deal

with him again, and there were investment bankers who weren't picking up his calls. A way would be found, however, to continue developing the blockchain technology. The company would go on. MacGregor shook his head. The whole thing was unfathomable. It was baffling. For no obvious reason Wright had found a way to disappear back into the shadows.

**Coda**

He seemed to miss me. Craig wanted to meet. It was a few weeks after the abortive 'reveal' and I saw when I got to Patisserie Valerie that he was happy again and ready to take on the world. 'It was unfair of me to request you not to publish certain things about our situation,' Ramona had written to me in an email. 'As you said, you have a debt to the truth, and that is as it should be.' And yet, as we all know, the truth has more faces than the town clock.

Wright told me in Patisserie Valerie that he felt free again. He had lost a third share in a billion dollars but he felt unburdened. He was sorry to have let good people down but now he could work in peace. Sherlock Holmes's central precept came into my mind. 'When you have eliminated the impossible, whatever remains, however improbable, must be the truth.'

'Do you want to know what I think?' I said to him after he told me again that all would be well from now on.

'Yes.'

'What if you were 30 per cent Satoshi. You were there at its formation and you were part of a brilliant group. You coded and you synthesised other people's work and you shared in the encryption keys. Then, some time in the last year, you upgraded yourself to 80 or 90 per cent. You were already a lot more Satoshi than anybody else has been hitherto, but the deal, in your eyes, required you to be more and in the end you couldn't carry that off.'

‘No,’ he said. And he flew off on a tangent about elliptical curves and the nature of the blockchain and how he never wanted to be a deity. I turned off my recording head at that point and stared through him.

Outside the café, he shook my hand. I knew I would never see him again. For six months we had allowed each other to think we were friends – subjects need storytellers, and storytellers need subjects. There had been a time when he’d imagined that I could free him from his fictions and build him a new story in reality. I was a willing stenographer, thinking Wright was something perhaps bigger than Satoshi. He was the internet’s habit of self-dramatisation and self-concealment all at once; its new sort of persona. What he actually did may never be known. Either he’s one of the greatest computer scientists of his generation, or he’s a reckless opportunist, or he’s both. We can’t be sure. But there he was, standing in Old Compton Street in the pouring rain, saying sorry.

# TAB 83-2

# EXHIBIT 2

From: **Ira K** [redacted]
Date: Tue, May 20, 2014 at 11:20 AM
Subject: Re: memory recall
To: Craig S Wright <craig@rcjbr.org>

Thanks. I guess the one he drew for me could have looked like that.

Wish I kept the card.

On Tue, May 20, 2014 at 3:25 AM, Craig S Wright <craig@rcjbr.org> wrote:
Neither of us were graphic artists …

**From:** Ira K [redacted]
**Sent:** Tuesday, 20 May 2014 5:03 PM
**To:** Craig Wright
**Subject:** Re: memory recall

i think the logo he drew for me only had only line going through the B, not two.

On Tue, May 20, 2014 at 3:01 AM, Craig Wright <craig@rcjbr.org> wrote:

We did partner ;)

The properties were not magnificent, but I loved them. In total I had a few cattle ranches and farm. Up in Port Macquarie. Wonderful beaches, but underdeveloped unlike Florida. In total about 550 acres.

I will have to see what I can dig up. The old Bitcoin logo we did is no longer used. I have a copy somewhere.

Some of the issues we still face come from how people assume making money must be counterfeit or otherwise illegal.

Craig

On 20/05/2014 4:53 pm, "Ira K" [redacted] wrote:
I thought I would share this memory of Dave I had.

I don't recall him ever saying the word Bitcoin to me, but I do
have a memory where I think he told me he was working on it.
We were visiting at my Dad's house I think for Thanksgiving, and
I believe it was the first time he met my daughter [redacted]. We started
talking about how successful Facebook had become and I asked
him if he was working on anything interesting. He told me he was
making his own money. I was like what? Are you making
counterfeit money? I thought maybe he was up to something fishy.
And then he said it was digital money and opened his wallet to
show me something like a business card with a logo on it.
But he couldn't find it so I think he just scribbled it on the back
of a card, the B with lines through it.

He also said he was doing some work with a rich foreign guy. I asked him
how rich is this guy? He said something like he's not super rich, but he owns
some properties. Then he said some other stuff about the foreign guy

that I don't remember. I replied to him saying why don't you partner with this guy. With your brains and his money you guys could create the next big thing like Facebook. He gave me a blank look and was silent, which I thought unusual for Dave to stop talking. Maybe he didn't want to directly come out and say you guys were already partners. Anyway, that's the only time I can recall where he mentioned this stuff to me.

I was wondering if you were aware of any business cards ever being printed with the Bitcoin logo on it. I never found any in his belongings. I wasn't sure if he was opening his wallet to show me a Bitcoin business card or if he just wanted to grab an existing card to draw the logo on the back of it.

Thanks,
Ira

From: **Craig S Wright** <craig@rcjbr.org>
Date: Tue, May 20, 2014 at 3:23 AM
Subject: RE: memory recall
To: Ira K [redacted]

Here you go – this is the first of the first.

The later version of the same

# TAB 83-3

# EXHIBIT 3

# Electronic Articles of Organization For Florida Limited Liability Company

L11000019904
FILED 8:00 AM
February 16, 2011
Sec. Of State
tcline

## Article I

The name of the Limited Liability Company is:

W&K INFO DEFENSE RESEARCH LLC

## Article II

The street address of the principal office of the Limited Liability Company is:

3119 CONTEGO LANE
PALM BEACH GARDENS, FL. US 33418

The mailing address of the Limited Liability Company is:

4371 NORTHLAKE BLVD #314
PALM BEACH GARDENS, FL. US 33410

## Article III

The purpose for which this Limited Liability Company is organized is:

ANY AND ALL LAWFUL BUSINESS.

## Article IV

The name and Florida street address of the registered agent is:

DAVID A KLEIMAN
3119 CONTEGO LANE
PALM BEACH GARDENS, FL. 33410

Having been named as registered agent and to accept service of process for the above stated limited liability company at the place designated in this certificate, I hereby accept the appointment as registered agent and agree to act in this capacity. I further agree to comply with the provisions of all statutes relating to the proper and complete performance of my duties, and I am familiar with and accept the obligations of my position as registered agent.

Registered Agent Signature: DAVE KLEIMAN

## Article V

L11000019904
FILED 8:00 AM
February 16, 2011
Sec. Of State
tcline

The name and address of managing members/managers are:

Title: MGRM
DAVID A KLEIMAN
4371 NORTHLAKE BLVD #314
PALM BEACH GARDENS, FL. 33410 US

## Article VI

The effective date for this Limited Liability Company shall be:

02/14/2011

Signature of member or an authorized representative of a member

Electronic Signature: DAVE KLEIMAN

I am the member or authorized representative submitting these Articles of Organization and affirm that the facts stated herein are true. I am aware that false information submitted in a document to the Department of State constitutes a third degree felony as provided for in s.817.155, F.S. I understand the requirement to file an annual report between January 1st and May 1st in the calendar year following formation of the LLC and every year thereafter to maintain "active" status.

# TAB 83-4

# EXHIBIT 4

FILED
4 NOV 2013
NA

Form 40 (version 2)
UCPR 35.1

# AFFIDAVIT OF Craig S Wright – 31st Oct 2013

| COURT DETAILS | |
|---|---|
| Court | NSW Supreme Court |
| Division | General Division Common Law |
| List | General |
| Registry | Sydney |
| Case number | 2013 / 225983 & |
| | 2013 / 245661 |

| TITLE OF PROCEEDINGS | |
|---|---|
| Plaintiff | **Craig Steven Wright (ABN 97 481 146 384)** |
| Defendant | **W&K INFO DEFENSE RESEARCH LLC** |

| FILING DETAILS | |
|---|---|
| Filed for | **Craig S Wright** |
| | Plaintiff |
| Contact name and telephone | Craig S Wright |
| | 0417 683 914 |
| Contact email | Craig S Wright (craigswright@acm.org) |

**AFFIDAVIT DETAILS**

| | |
|---|---|
| Name | Craig S Wright |
| Address | 43 St Johns Ave Gordon |
| Occupation | Director / Lecturer |
| Date | ~~31 Oct 2013~~ 4th November 2013 |

I affirm:

1. I am the plaintiff.

2. I believe that the information contained in this affidavit is true.

3. The defendant is indebted to the plaintiff in respect of the balance of the cause of action 2013 / 225983 for which this action was commenced in the amount of **$**28,254,666.00 together with interest on the principal sum from the date of the cause of action to today's date of **$156,755.34** calculated as follows:

| Period | Days & Rate p.a. | Debt Amount | Interest |
|---|---|---|---|
| 25 Jul 2013 – 23 Aug 2013 | 93 days @ 6.750% | $28,254,666.00 | $488,637.81 |
| $5,254.17 per day until entry of judgment | | | |
| | | Total: | $28,743,303.81 |

4. The defendant is indebted to the plaintiff in respect of the balance of the cause of action 2013 / 245661 for which this action was commenced in the amount of **$**28,254,666.00 together with interest on the principal sum from the date of the cause of action to today's date of **$156,755.34** calculated as follows:

| Period | Days & Rate p.a. | Debt Amount | Interest |
|---|---|---|---|
| 25 Jul 2013 – 23 Aug 2013 | 93 days @ 6.750% | $28,534,049.79 | $490,746.57 |
| $5,254.17 per day until entry of judgment | | | |
| | | Total: | $29,024,796.36 |

5. Since the commencement of this action no payments have been made or credits accrued.

6. The amount for filing, issuing and serving of the statement of claim herein, ~~which~~ has not been paid is **$0**.

7. The amount of solicitor's costs calculated in accordance with the Local Courts (Civil Claims) Rules, which has not been paid is $0.

8. The Statement of Claim was served on the defendant on 26 Jul 2013 by leaving it with the Defendant at the registered address for service of:

David A Kleiman
3119 Contego Lane
Palm Beach Gardens
Fl 33410 USA

9. The Statement of Claim was served on the defendant on 26 Jul 2013 by mailing it with the Defendant at the registered mailing address for service of:

David A Kleiman
4371 Northlake Blvd #314
Palm Beach Gardens
Fl 33410 USA

10. The defendant is a US LLC based in Florida USA. The US resident director was David A Kleiman. (Appendix A).

11. The market rate (at this date) for the contract quantity of Bitcoin (Currency Code XBT) on Xe.com is $AUD 67,863,954.23 at a market rate of 1 XBT = 226.213 AUD
1 AUD = 0.00442061 XBT.

12. A contract was formed in April 2011 (Appendix B).

13. 300,000 Bitcoin and a series of software projects was to be paid in 2013 as consideration for this agreement.

14. On 02 Feb 2013 the agreement to pay the 300,000 Bitcoin was noted in an email of Dave Kleiman to Craig Wright noting the verbal agreement to start a Bitcoin exchange based on the mined Bitcoin of Mr Kleiman and the returned amounts paid as consideration.

15. The company, COIN-EXCH PTY. LTD. ACN 163 338 467 was started on 17th Apr 2013 with an agreement for Mr Kleiman to transfer the remaining capital from the contract (B) in repayment as well as to inject a further amount of capital into the company on or before 30th April 2013 Appendix D).

16. The contract was associated with an invoice to be paid for $34,862,323.00 USD from 22Apr 2011. This was paid in full.

17. Mr David A Kleiman died on 26th April 2013 (US time) (Appendix F).

18. The transfers made into "W&K Info Defence LLC" (Appendix G) were completed in April 2013. These are pseudo anonymous but public. The details have been supplied in Appendix G. Details of these transactions have been given to the Australian Tax Office for tax purposes.

19. The Bitcoin addresses used have been independently validated by NSW Solicitors under oath (Appendix H).

20. Work and research was conducted under the US Dept. of Homeland Security DHS BAA

    (a) Appendix I

    (b) Appendix J

    (c) Appendix K

21. Mr Kleiman noted that screening software was developing in unwarranted manners and I noted that our software was looking at being better in an email (Appendix L).

22. The coversheets for the S&T Directorate projects are included in Appendix M

23. On 01st August 2013 a shareholders meeting was called for "W&K Info Defense LLC" to be held on the 16th August 2013. The meeting was emailed to the company address as well as send to the address of the shareholders and company. The shareholding of "W&K Info Defense LLC" was:

| | | |
|---|---|---|
| 1. | Craig S Wright | 50.0 % |
| 2. | David A Kleiman | 50.0 % |

24. The meeting from point 23 meeting was held on the 16th of August 2013. The following people were present:

    1. Jamie Wilson
    2. Craig S Wright

25. "W&K Info Defense LLC" was an incorporated partnership. All shares are held jointly. The constitution states there is to be a resident US director. Shares were held jointly as per the US Companies Act, 1956.

26. The following points were moved at the meeting:

1. Jamie Wilson will act as director for the purposes of consenting to orders and the company to be wound down.

2. The vote was Craig Wright – "Yes". No other parties.

3. It was agreed that following the motion to accept the debt owed by the company (W&K Info Defense LLC), it would be closed.

27. Projects for the development of software started in 2009 under a company named "Integyrs Pty Ltd" (Appendix N).

28. The development of the software was extended considerably in the period between 2011 – 2013.

29. I discovered that Mr Kleiman died before transferring the required funds on the 29th April 2013. The payment was planned for 30th April 2013.

30. Mr Kleiman was not added as a shareholder and director of Coin-Exch Pty Ltd as was planned to occur on the 30th Apr 2013 as a consequence.

AFFIRMED at ~~Gordon, NSW~~ Sydney

Signature of deponent

Name of witness NICHOLAS CHARLES MCDONALD

Address of witness 21/103 MAJORS BAY ROAD CONCORD NSW 2137

Capacity of witness JUSTICE OF THE PEACE

And as a witness, I certify the following matters concerning the person who made this affidavit (the **deponent**):

1 ~~I saw the face of the deponent.~~ *[OR, delete whichever option is inapplicable]* I saw the face of the deponent

2 I have confirmed the deponent's identity using the following identification document:

NSW DRIVERS LICENCE

Identification document relied on (may be original or certified copy)[1]

Signature of witness

Note: The deponent and witness must sign each page of the affidavit. See UCPR 35.7B.

NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174
In and for the State of New South Wales, Australia
21/103 Majors Bay Rd
Concord NSW 2137
Telephone 02 96034779 / 0412473 696

[1 "Identification documents" include current driver licence, proof of age card, Medicare card, credit card, Centrelink pension card, Veterans Affairs entitlement card, student identity card, citizenship certificate, birth certificate, passport or see Oaths Regulation 2011 or JP Ruling 003 - Confirming identity for NSW statutory declarations and affidavits, footnote 3.]

A.

# Electronic Articles of Organization For Florida Limited Liability Company

L11000019904
FILED 8:00 AM
February 16, 2011
Sec. Of State
tcline

## Article I

The name of the Limited Liability Company is:

W&K INFO DEFENSE RESEARCH LLC

## Article II

The street address of the principal office of the Limited Liability Company is:

3119 CONTEGO LANE
PALM BEACH GARDENS, FL. US 33418

The mailing address of the Limited Liability Company is:

4371 NORTHLAKE BLVD #314
PALM BEACH GARDENS, FL. US 33410

## Article III

The purpose for which this Limited Liability Company is organized is:

ANY AND ALL LAWFUL BUSINESS.

## Article IV

The name and Florida street address of the registered agent is:

DAVID A KLEIMAN
3119 CONTEGO LANE
PALM BEACH GARDENS, FL. 33410

Having been named as registered agent and to accept service of process for the above stated limited liability company at the place designated in this certificate, I hereby accept the appointment as registered agent and agree to act in this capacity. I further agree to comply with the provisions of all statutes relating to the proper and complete performance of my duties, and I am familiar with and accept the obligations of my position as registered agent.

Registered Agent Signature: DAVE KLEIMAN

This is the annexure marked with the letter 'A' referred to in the Affidavit / Affirmation / ~~Statutory Declaration~~ of Craig S WRIGHT sworn/affirmed/~~declared~~ before me at Sydney on the 4th day of November 2013

~~One page only~~
Page 1 of 2 pages

NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174

A

L11000019904
FILED 8:00 AM
February 16, 2011
Sec. Of State
tcline

## Article V

The name and address of managing members/managers are:

Title: MGRM
DAVID A KLEIMAN
4371 NORTHLAKE BLVD #314
PALM BEACH GARDENS, FL. 33410 US

## Article VI

The effective date for this Limited Liability Company shall be:

02/14/2011

Signature of member or an authorized representative of a member

Electronic Signature: DAVE KLEIMAN

I am the member or authorized representative submitting these Articles of Organization and affirm that the facts stated herein are true. I am aware that false information submitted in a document to the Department of State constitutes a third degree felony as provided for in s.817.155, F.S. I understand the requirement to file an annual report between January 1st and May 1st in the calendar year following formation of the LLC and every year thereafter to maintain "active" status.

# INTELLECTUAL PROPERTY LICENCE FUNDING AGREEMENT

B

PARTIES

Craig Wright R&D
ABN 97 481 146 384
(Financer)

AND

W&K Info Defense LLC
(Provider)

This is the annexure marked with the letter 'B' referred to in the Affidavit / Affirmation / Statutory Declaration of Craig SWRIGHT sworn/affirmed/declared before me at Sydney on the 4th day of November 2013

One page only
Page 1 of 14 pages

NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174

Ref: CEWK01

K C

**THIS DEED** dated 22nd day of April 2011

**BETWEEN**

Craig Wright of Craig Wright R&D

(Financer)

And

Dave Kleiman for W & K Info Defense LLC

(Provider)

**RECITALS**

**A.** The Financer controls the following Bitcoin (BTC) addresses:

(a) 12hRmmSda9qSSEH656zBaKEbeisH6ZhdTm.

(b) 12C9c9VQLMrLi4Ffzq2wDvwrKnUPaAaNFp.

**B.** The Provider desires the intellectual property for the permitted use and to extend this for other purposes desirable to both parties.

**C.** The Provider will use the funding for the development of several software products.

**D.** The provider will return the loaned finances (in Bitcoin) on or before 01 July 2013 and 30 Dec 2013.

**E.** The Provider will remain completely confidential on all matters in this deed (including even that family members do not have knowledge of the transaction).

**F.** The financer will send the following amounts (in Bitcoin) to to following address by 30 April 2011:

(a) 165,140 BTC

(b) 1MSUvGS9BEjpL35CKu7feF4HaPCXv2cht7

**G.** The financer will send the following amounts (in Bitcoin) to toe following address by 30 August 2011:

(a) 50,000 BTC

(b) 1JjtxXmbC95sgn5kE2Hm92axA7hcbDkRhK

**H.** The Financer and the Provider wish to record the licence, which has been granted to the Provider to use the intellectual property in accordance with this deed.

**I.** The Financer is the absolute owner of the entire unencumbered copyright in the works described in the schedule when complete.

**J.** The Financer has agreed to license the works to the Provider and the Provider has agreed to accept such licence on the following terms and conditions.

**K.** The provider will fund the software development using Bitcoin.

**L.** The Financer will provide 1,024 core Xeon and GPU based hardware solution.

(a) It is acknowledged that two SGI ICE XE310 – 512 core hosts have been provided and are in a data centre specified by the provider

(b) The provider will use these systems to mine Bitcoin

(c) The provider expects to earn 12,000 BTC per month using these systems for the period to 30 June 2013

(d) The systems will be hosted in the US at a facility managed by the provider.

**M.** The provider will pay for the use of the systems and the loan as follows:

(a) 250,000 BTC to be repaid on 30 June 2013

(b) 50,000 BTC to be repaid on 30 Dec 2013

(c) The developed software will be exclusively licensed perpetually to the financer (as of 30 June 2013).

(d) The software may be used but not distributed by the provider.

**N.** The contract is complete when 300,000 BTC have been repaid.

**O.** It is agreed that the value of the loan to be repaid is $ AUD 20,000,000 in two parts (for a total of $40,000,000).

**P.** The server systems will return to the Financer at the completion of the contract.

**Q.** On default, the contract is to be repaid in full to the financer.

OPERATIVE PART

1. **Definitions**

In this deed:

(a) Business means the business operated by the Provider described as such in the schedule;

(b) Business day means a day, not being a Saturday, Sunday or gazetted public holiday, on which banks are open for commercial business where performance of an obligation under this deed is to take place;

(c) Claim means, in relation to a person, a claim, demand, remedy, suit, injury, damage, loss, cost liability, action, proceeding, right of action, chose in action, claim for compensation or reimbursement or liability incurred by or to be made or recovered by or against the person, however arising and whether ascertained or unascertained, or immediate, future or contingent;

(d) Commencement date means the date so specified in the schedule;

(e) Confidential information means all technical and other information and know how, including all information and know how in any eye or machine readable form or other format, disclosed or given to the Provider from any source in respect of or incidental to:

(i) The product;

(ii) The technology;

(iii) The Financer; and

(iv) Any other information disclosed or given to the Provider by the Financer which is declared by the Financer to be confidential information;

(f) Improvements means any improvement, modification, enhancement or derivative of the intellectual property arising during the term;

(g) Intellectual property means:

(i) The confidential information;

(ii) The improvements;

(iii) The patent; and

(iv) The trade mark;

(h) Licence fee means the amount calculated and paid by the Provider to the Financer specified in the schedule;

(i) Notice means a written notice, consent approval, direction, order or other communication;

(j) Obligation means any legal, equitable, contractual, statutory or other obligation, deed, covenant, commitment, duty, undertaking or liability;

(k) Patent means the registered patent or patent application including the provisional and complete specifications described in the schedule;

(l) Permitted use means to conduct the business to exploit market, promote, develop, integrate, research, sell and conduct and any other activity undertaken with respect to the product for profit or reward;

(m) Product means the product described as such in the schedule;

(n) Right includes a legal, equitable, contractual, statutory or other right, power, authority, benefit, privilege, remedy, discretion or cause of action;

(o) Technology means all that technical information which relates to or forms part of the product, including, without limitation, methodology, techniques, drawings, outlines, notes, algorithms, detailed designs, flow charts, results, software: partial or intermediate versions and prototypes, data, formulae and other proprietary information and know how in the Provider's possession or control or which is revealed to the Provider which relates to the product;

(p) Term means the term set out in the schedule; and

(q) Trade mark means the registered trade mark, trade mark registration application and common law trademarks described in the schedule.

**2. Interpretation**

This deed is governed by the law of NSW and the parties submit to the non-exclusive jurisdiction of the courts of that state.

In the interpretation of this deed:

(a) References to legislation or provisions of legislation include changes or re-enactments of the legislation and statutory instruments and regulations issued under the legislation;

(b) Words denoting the singular include the plural and vice versa; words denoting individuals or persons include bodies corporate and vice versa; references to documents or deeds also mean those documents or deeds

as changed, novated or replaced, and words denoting one gender include all genders;

(c) Grammatical forms of defined words or phrases have corresponding meanings;

(d) Parties must perform their obligations on the dates and times fixed by reference to the schedule;

(e) Reference to an amount of money is a reference to the amount in the lawful currency of the Commonwealth of Australia;

(f) If the day on or by which anything is to be done is a Saturday, a Sunday or a public holiday in the place in which it is to be done, then it must be done on the next business day;

(g) References to a party are intended to bind their executors, administrators and permitted transferees; and

(h) Obligations under this deed affecting more than one party bind them jointly and each of them severally.

**3. Licence**

The Financer hereby grants to the Provider an exclusive licence to use the intellectual property for the permitted use on the terms of this deed.

In consideration of the licence fee payable hereunder the Financer grants to the Provider an exclusive transferrable licence to copy publish sell or otherwise use the works in the course of its business in Australia and/or Overseas in respect of the whole or any part of the works commencing on 01st July 2013.

In consideration of the licence hereby granted to the Provider the Provider must pay a one off licence fee of $20,000,000 (GST exclusive) to the Financer on or before the 30th June 2013. The provider will also transfer the designated account of the provider:

(a) 250,000 BTC to be repaid on 30 June 2013

(b) 50,000 BTC to be repaid on 30 Dec 2013

The payment is to be issued in Bitcoin as per the schedule.

**4. Provider's promises**

(a) **Undertakings**

The Provider undertakes to:

(i) Use its reasonable commercial endeavours to:

(1) Preserve the value and validity of the intellectual property; and

(2) Create, promote, retain, and enhance the goodwill in the intellectual property;

(ii) During the term and thereafter the termination of this deed not to allow or facilitate the use, nor exploit the intellectual property in a manner in any way detrimental to the Financer and not contravene, deny or contest the rights subsisting in the intellectual property, and take such steps as may be appropriate and available to the Provider to prevent the infringement of any and all the rights subsisting in the intellectual property;

(iii) In connection with the permitted use not give any warranty:

(1) Beyond that which the Provider is obliged in law to give; or

(2) Which has not been approved in writing by the Financer;

(iv) To use the intellectual property only for the permitted use and not for any other use;

(v) Treat as confidential the confidential information except that which at the time of its disclosure to the Provider was generally available, or subsequently became known to the public provided always that this covenant shall continue in full force and effect notwithstanding that this deed has terminated; and

(vi) Devote all reasonable commercial endeavours in the conduct and operation of the business.

(b) **Indemnity**

(i) The Provider hereby agrees to fully, effectually, and promptly indemnify the Financer against any loss, either direct or indirect, damage or expense whatsoever which the Financer may suffer or incur in respect of:

(1) Any breach by the Provider of the provisions of this deed; or

(2) Any claim by any person against the Financer arising out of or in respect of the exploitation of the intellectual property by the Provider; and

(ii) The Provider hereby irrevocably releases the Financer and waives all claims which the Provider may have in the future against the Financer, in respect of any action claim or remedy whatsoever in any way attributable to the exploitation of the intellectual property by the Provider.

**5. Improvements**

If the Provider develops any improvements, the Financer hereby irrevocably:

(a) Grants to the Provider the right to apply for any incidental intellectual property rights available in respect of that improvement and in connection with such application, the Financer shall:

(i) Make, supply and assist in the preparation of all models, plans, drawings or specifications necessary or convenient for the proper understanding or development of the improvements; and

(ii) Grant and do all things necessary to give effect to an assignment of the intellectual property rights in respect of the improvements to the Provider;

(b) Assigns, transfers and sets over absolutely to the Provider all right title and interest to the improvements including all claims as they relate to the improvements.

**6. GST**

(a) GST means a goods and services tax as defined in A New Tax System (Goods and Services Tax) Act 1999.

(b) In respect of any taxable supply, the Provider must pay to the Financer an additional amount equal to the prevailing GST rate on the supply. The additional amount referred to in this clause is payable at the same time and in the same manner as the licence fee subject to the receipt by the Provider of a valid tax invoice, as defined in A New Tax System (Goods and Services Tax) Act 1999.

7. **Term and termination**

(a) **Term**

This deed begins on 01st July 2018 the commencement date and will continue for the term unless it is earlier terminated.

(b) **Termination on notice**

Either party may terminate this deed by notice in writing to the other if the other party commits any breach of any provision of this deed, and has failed to remedy such breach within fourteen days of receipt of notice specifying:

(i) The exact nature of the breach committed by the defaulting party; and

(ii) What is required by the defaulting party to remedy the breach;

8. **Licence fee**

(a) **Payment of licence fee**

The Provider must pay the licence fee specified in the schedule to the Financer during the term.

(b) **Late payment**

If the licence fee or any other monies payable by the Provider to the Financer remain unpaid for seven days after the due date for payment, whether or not formal demand has been made, then the Provider shall pay, in addition to any monies actually owing to the Financer, interest at the rate of 2% over the bank indicator lending rate nominated by the Financer on such monies from the date the payment actually fell due until such monies are recovered and paid to the Financer.

9. **Warranties by Financer**

The Financer warrants to the Provider that:

(a) The Financer has the power and authority to enter into this deed; and

(b) The intellectual property rights granted under this deed will not when used in accordance with this deed infringe the intellectual property rights of any person.

**10. Third party claim**

(a) Provided that the Provider is not in breach of its obligations under this deed, if a third party makes a claim against the Provider alleging that use of the intellectual property infringes its intellectual property rights, the Financer will defend, indemnify and hold harmless the Provider from such a claim provided that the:

(i) The Provider notifies the Financer in writing promptly of the claim;

(ii) The Provider provides such information, assistance and co-operation as the Financer may reasonably request and at its expense, from time to time; and

(iii) The Financer has full discretion to defend, compromise or settle any such claim on such terms as the Financer deems fit.

(b) If the Financer cannot satisfactorily settle the claim so as to retain ownership of the intellectual property, its liability will be limited to terminating this deed, and refunding the Provider an amount equal to the portion of any licence fee paid for the period following termination.

(c) Nothing in this clause authorises the Provider to defend, compromise or settle any claim on the Financer's behalf.

**11. Limitation of liability**

(a) Other than in respect of a party's:

(i) Breach of the confidentiality provisions of this deed; or

(ii) Infringement of another party's intellectual property rights; or

(iii) Indemnification obligations under this deed; or

(iv) Wilful misconduct.

(b) Neither party will be liable to the other for any consequential, special or punitive damages arising out of this deed. Each party's cumulative direct damages will be limited to the licence fee payable under this deed in the prior twelve month period. This clause survives the termination or expiration of this deed.

**12. Assignment**

No party may assign its rights or obligations under this deed without the prior written consent of the other parties, which consent may be given or withheld, or given on conditions, in the absolute discretion of those other parties.

**13. Time**

The parties hereto agree that time shall in all respects be of the essence in regards this deed.

**14. Notices**

A communication required by this deed, by a party to another, must be in writing and may be given to them by being:

(a) Delivered personally; or

(b) Posted to their address specified in this deed, or as later notified by them, in which case it will be treated as having been received on the second business day after posting; or

(c) Faxed to the facsimile number of the party with acknowledgment of receipt received electronically by the sender, when it will be treated as received on the day of sending, or

(d) Sent by email to their email address, when it will be treated as received on that day.

**15. Waiver or variation**

(a) A party's failure or delay to exercise a power or right does not operate as a waiver of that power or right.

(b) The exercise of a power or right does not preclude:

(i) Its future exercise; or

(ii) The exercise of any other power or right; or

(iii) The variation or waiver of a provision of this deed or a party's consent to a departure from a provision by another party will be ineffective unless in writing executed by the parties.

**16. Counterpart**

This deed may be executed in any number of counterparts each of which will be an original, but counterparts together will constitute one and the same instrument, and the date of the deed will be the date on which it is executed by the last party.

**17. Costs**

(a) Each party will pay its own costs of and incidental to this deed.

(b) The Provider will bear all duty payable on this deed and keep indemnified the Financer in respect of that liability.

(c) The Provider will bear all GST payable in respect of any supply under this deed upon receipt of tax invoice issued by the Financer.

**18. Escrow**

(a) The paper Bitcoin Wallet with address 1933phfhK3ZgFQNLGSDXvqCn32k2buXY8a will be held by the financer as assurance or the contract and will convert to the ownership of the financer on default of the provider.

(b) All source code and agreements are to be held in a manner that the financer can access on default.

REFERENCE SCHEDULE

| | |
|---|---|
| **Deed date:** | 01st April 2011 |
| **Licence fee:** | (a) 250,000 BTC to be repaid on 30 June 2013<br>(b) 50,000 BTC to be repaid on 30 Dec 2013<br>(ex GST) for exclusive perpetual assignment |
| **Product:** | Bitcoin and Exchange Software in C/C++/C#/R code |
| **Commencement date:** | 01st July 2011 |
| **Term:** | Two (2) years |
| **Trademark:** | All Marks Associated with C01N and associated marks<br>To be filed |
| **Patent:** | All IP under BAA-001 / 002 / 003 / 004 |

**SIGNED AS A DEED**

Executed by
W & K Info Defense LLC )
in accordance with s.127 )
Corporations Act 2001 (CTH) and its constitution )

Dave Kleiman

Dave Kleiman
DIRECTOR

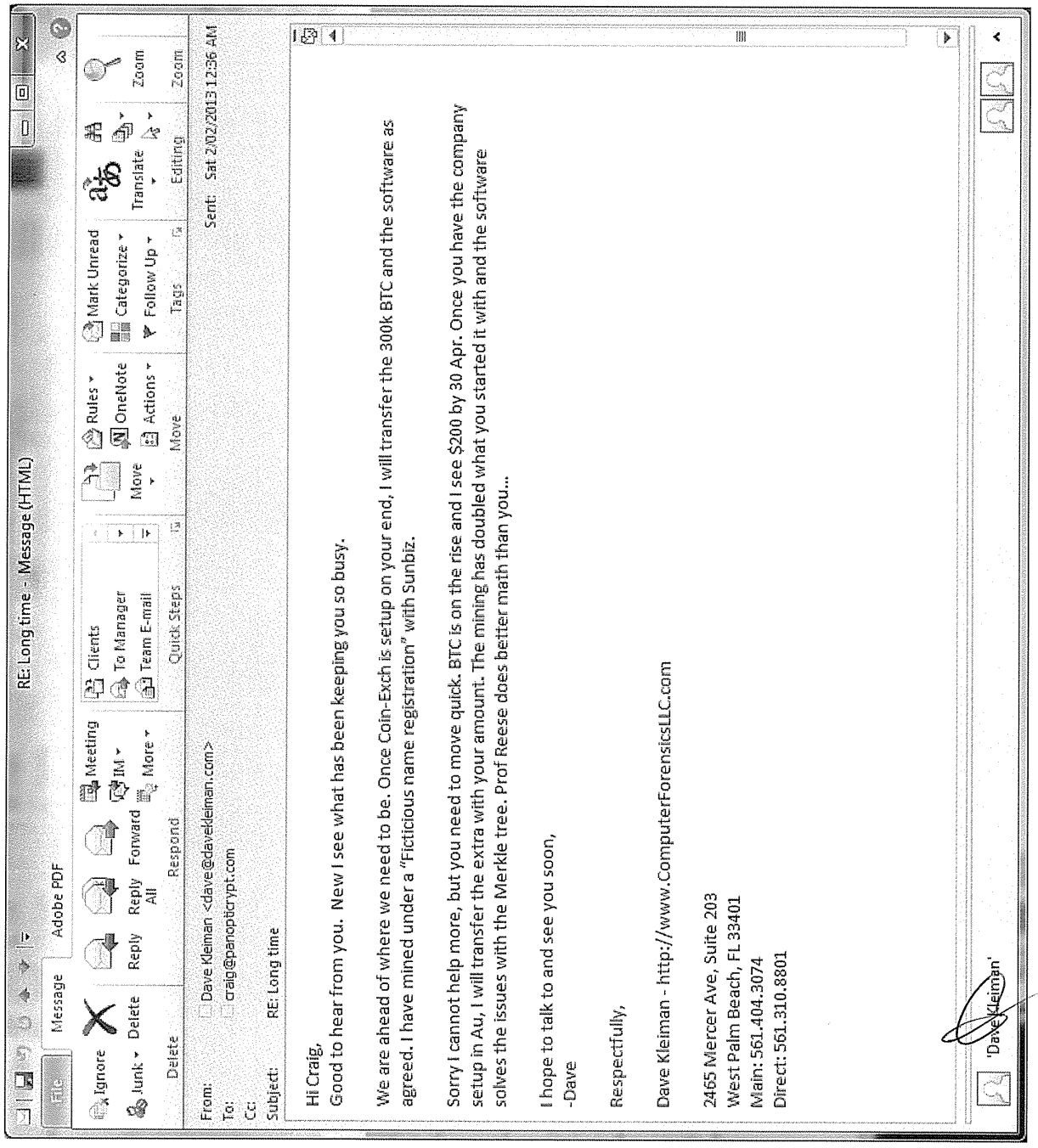
Executed by
Craig Wright R&D (A.B.N. 97 481 146 384)

Craig S Wright

This is the annexure marked with the letter C referred to in the Affidavit / ~~Affirmation / Statutory Declaration~~ of Craig S WRIGHT
~~sworn/affirmed/declared~~ before me at Sydney
on the 4th day of November 2013

One page only
Page 1 of 1 pages

NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174



**ASIC**
Australian Securities & Investments Commission

**Forms Manager**
Company Officeholders

**Company:** COIN-EXCH PTY. LTD. ACN 163 338 467

## Company details

| | |
|---|---|
| Date company registered | 17-04-2013 |
| Company next review date | 17-04-2014 |
| Company type | Australian Proprietary Company |
| Company status | Registered |
| Home unit company | No |
| Superannuation trustee company | No |
| Non profit company | No |

### Registered office

LEVEL 5 , 32-38 DELHI ROAD , MACQUARIE PARK NSW 2113

### Principal place of business

LEVEL 5 , 32-38 DELHI ROAD , MACQUARIE PARK NSW 2113

### Officeholders

WRIGHT, CRAIG STEVEN

Born 23-10-1970 at BRISBANE QLD

43 ST JOHNS AVENUE , GORDON NSW 2072

Office(s) held: Director, appointed 17-04-2013
Secretary, appointed 17-04-2013

This is the annexure marked with the letter "D" referred to in the Affidavit/Affirmation/Statutory Declaration of CRAIG S WRIGHT sworn/affirmed/declared before me at Sydney on the 4th day of December 2017

One page only
Page 1 of 1 pages

NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174

### Company share structure

| Share class | Share description | Number issued | Total amount paid | Total amount unpaid |
|---|---|---|---|---|
| FOU | FOUNDERS | 21500000 | 21500000.00 | 0.00 |
| ORD | ORDINARY | 20000000 | 20000000.00 | 0.00 |

### Members

PANOPTICRYPT PTY LTD — 43 ST JOHNS AVENUE , GORDON NSW 2072

| Share class | Total number held | Fully paid | Beneficially held |
|---|---|---|---|
| ORD | 17000000 | Yes | No |

DENARIUZ SG — 108 NAMLY AVE , SINGAPORE , SINGAPORE

| Share class | Total number held | Fully paid | Beneficially held |
|---|---|---|---|
| ORD | 3000000 | Yes | Yes |

WRIGHT , CRAIG STEVEN — 43 ST JOHNS AVENUE , GORDON NSW 2072

| Share class | Total number held | Fully paid | Beneficially held |
|---|---|---|---|
| FOU | 21500000 | Yes | No |

# INVOICE

E

Date: 4/22/2011
Invoice # 1253

W&K INFO DEFENSE RESEARCH
LLC
4371 NORTHLAKE BLVD #314
PALM BEACH GARDENS
FL 33410
561.310.8801
dave@davekleiman.com

Craig Wright R&D
ABN 97 481 146 384
51 Cowangarra Rd
Bagnoo NSW 2446
+61 417 683 914
Customer ID CWR001

Craig Wright R&D
ABN 97 481 146 384
51 Cowangarra Rd
Bagnoo NSW 2446
+61 417 683 914
Customer ID CWRD01

| Salesperson | Job | Shipping Method | Shipping Terms | Delivery Date | Payment Terms | Due Date |
|---|---|---|---|---|---|---|
| Dave A Kleiman | BAA 001 | Software | NA | By Contract | Due on receipt | 30 Apr 2011 |

| Qty | Item # | Description | Unit Price | Discount | Line Total |
|---|---|---|---|---|---|
| 165,140 | Bitcoin | BTC loan @ USD 0.88 | 0.88 | | 145,323 |
| 50,000 | Bitcoin | BTC loan @ USD 0.88 | 0.88 | | 44,000 |
| 2 | SGI System | SGI ICE XE310 lease | 4,411,500 | | 8,823,000 |
| 1 | Software | Per agreement | 20,000,000 | | 20,000,000 |
| | BAA-001 | BAA 11-02-TTA 01-0127-WP | 650,000 | | 650,000 |
| | BAA-002 | BAA 11-02-TTA 09-0049-WP | 2,200,000 | | 2,200,000 |
| | BAA-003 | BAA 14-02-TTA 01-0025-WP | 1,200,000 | | 1,200,000 |
| | BAA-004 | BAA 11-02-TTA 01-0127-WP | 1,800,000 | | 1,800,000 |

**Total Discount**

| | |
|---|---|
| **Subtotal** | 34,862,323 |
| **Sales Tax** | |
| **Total** | 34,862,323 |

Terms in CEWK01

*Advanced security and research*

*Thank you for your business!*

This is the annexure marked with the letter E referred to in the Affidavit / Affirmation / Statutory Declaration of Craig S WRIGHT sworn/affirmed/declared before me at Surfers on the 4th day of November 2018

One page only
Page 1 of 1 pages

NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174

# Dave Kleiman

From Wikipedia, the free encyclopedia

**Dave Kleiman** (1967 - 2013)[1] was a noted Forensic Computer Investigator, an author/coauthor of multiple books and a noted speaker at security related events.[2][3][4]

| Dave Kleiman | |
|---|---|
| **Born** | 1967<br>U.S. |
| **Died** | April 26, 2013<br>Palm Beach Gardens, Florida |
| **Occupation** | Forensic Computer Investigator |
| **Website** | http://www.davekleiman.com/ |

## Contents



This is the annexure marked with the letter "F" referred to in the Affidavit / ~~Affirmation / Statutory Declaration of~~ CRAIG WRIGHT
~~sworn/affirmed/declared~~ before me at Soho
on the 4th day of November 2018

~~One page only~~
Page 1 of 4 ~~pages~~

NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174

## Computer security & forensics

For a number of years in the 1990s, Kleiman was a sworn law enforcement officer for the Palm Beach County Sheriff's Office (PBSO).[3][4] While there, he attained the rank of detective. Also, while at the PBSO, he worked as a System Security Analyst in the Computer Crimes Division and also helped set up the Computer Forensics Lab.[3][4]

Dave Kleiman is a regular contributor to a wide array of online forums and mailing lists where he assists network engineers and other IT professionals of varying levels in solving their issues, regardless of the level of difficulty involved. Kleiman is also well known as an advisor to engineering professionals in numerous industries.[2][3][4]

Dave also regularly volunteers his time and expertise assisting local and federal law enforcement agencies in cases both domestic and international in scope.

He is the creator of the "one-shot server lockdown utility" S-lok for Microsoft Windows servers.[3][4]

On January 1, 2007 he was named Microsoft MVP for Windows - Security

## Publications

- Co-author: Microsoft Log Parser Toolkit; Syngress Publishing; ISBN 1-932266-52-6
- Co-author: Security Log Management: Identifying Patterns in the Chaos; Syngress Publishing; ISBN 1-59749-042-3
- Technical editor: Perfect Passwords: Selection, Protection and Authentication; Syngress Publishing; ISBN 1-59749-041-5
- Technical editor: Winternals Defragmentation, Recovery, and Administration Field Guide; Syngress Publishing; ISBN 1-59749-079-2
- CD and DVD Forensics: Technical Editor, ISBN 1-59749-128-4
- How to Cheat at Windows System Administration: Contributing Author, ISBN 1-59749-105-5
- Enemy at the Water Cooler: Real Life Stories of Insider Threats, Technical Reviewer, ISBN 1-59749-129-2
- Rootkits for Dummies: Technical editor, ISBN 978-0-471-91710-6
- Windows Forensic Analysis Including DVD Toolkit: Technical Editor, ISBN 1-59749-156-X
- The Official CHFI Study Guide (Exam 312-49): Co-Author, ISBN 1-59749-197-7

## References


1. ^ "Obituary: Former PBSO deputy dies in his home" (http://www.mypalmbeachpost.com/news/news/local/obituary-former-pbso-deputy-dies-in-his-home/nXcqR/). Palm Beach Post. Retrieved May 1, 2013.
2. ^ *a b* "SANS WhatWorks Summit in Forensics and Incident Response" (http://www.sans.org/forensics09_summit/speakers.php#kleiman). SANS.
3. ^ *a b c d e* "Dave Kleiman" (http://credencecorp.com/bios/DaveKleiman.html). CredenceCorp.

4. ^ a b c d e "Dave Kleiman" (http://www.oreillynet.com/pub/au/2560?x-t=book.view). O'Reilly.

## External links

- Dave Kleiman's personal web site (http://www.davekleiman.com)
- Palm Beach County Sheriff's Office (http://www.pbso.org)
- CastleCops (http://www.castlecops.com)
- Microsoft MVP Program (https://mvp.support.microsoft.com/mvpexecsum)
- Microsoft MVP profile (https://mvp.support.microsoft.com/profile=C4ED32CD-9982-45F2-8636-BDE271C0DAC2)

Retrieved from "http://en.wikipedia.org/w/index.php?title=Dave_Kleiman&oldid=553157307"
Categories: 1967 births | 2013 deaths | People associated with computer security

**Craig S Wright**

| | |
|---|---|
| **From:** | Carter Conrad <carter@computerforensicsllc.com> |
| **Sent:** | Tuesday, 30 April 2013 1:23 AM |
| **To:** | Patrick Paige |
| **Cc:** | Bill Long; Greg Kelley; Craig Ball; Matthew Shannon; Jerry Hatchett; Eric Robi; Greg Freemyer; Paul Henry; Craig S. Wright; Scott Moulton'; Wayne Marney; Bob Bell; Bill Dean; Kimon Andreou; Greg Kelley |
| **Subject:** | Dave Kleiman |

As close friends of Dave, Patrick and I wanted to let you know in advance of any general posting that we have lost a dear friend and colleague…
As most of you are aware Dave was battling an infection from 2010, and had never fully recovered in the 2 ½+ years that followed.
Dave died in his home in Palm Beach Gardens of, what is being told to us, natural causes.
At this time no further details are available, although there are plans for a memorial, and these will be pasted on as they become available.

Carter V Conrad, Jr
Computer Forensics, LLC
1880 N. Congress Avenue, Suite 333
Boynton Beach, Florida 33426
Phone: (561) 404-3074
Cell: (561) 502-3935

www.ComputerForensicsLLC.com





# Bitcoin Address

**Summary**

| | |
|---|---|
| Address | 12hRmmSda9qSSEH656zBaKEbeisH6ZhdTm |
| Short Link | http://blockchain.info/fb/12hrmm |
| Tools | Taint Analysis - Related Tags - Unspent Outputs |

This is the annexure marked with the letter G referred to in the Affidavit / Affirmation / Statutory Declaration of CRAIG S WRIGHT sworn/affirmed/declared before me at Soho on the 4th day of November 2013
One page only
Page 1 of 8 pages
NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174

**Transactions**

| | |
|---|---|
| No. Transactions | 2 |
| Total Received | $ 74,055,693.41 |
| Final Balance | $ 0.00 |

Request Payment | Donation Button

## Transactions

Filter

ddb352955903db83f76edb85f2121c51859b2f41a3...

2011-08-27 02:29:26

1PWr5e1JjL8wy6uzKzb5d3pCxkNLYm5vt1
1JjtxXmbC95sgn5kE2Hm92axA7hcbDkRhK

$ 74,055,693.41

796187f76168cd0ca2fff6c3f967fe28242429cec320e...

2011-08-27 02:29:26

12hRmmSda9qSSEH656zBaKEbeisH6ZhdTm

$ 74,055,693.41

Home Charts Stats Wallet

# Bitcoin Address

## Summary

| | |
|---|---|
| Address | 1MSUvGS9BEjpL35CKu7feF4HaPCXv2cht7 |
| Short Link | http://blockchain.info/fb/1msuv |
| Tools | Taint Analysis - Related Tags - Unspent Outputs |

## Transactions

| | |
|---|---|
| No. Transactions | 2 |
| Total Received | $ 36,551,156.21 |
| Final Balance | $ 0.00 |

Request Payment Donation Button

## Transactions

Filter

0121f30f11152b3df11904401e13b1b972a5408682...

2011-04-29 03:20:56

1B4JfdD4jGUWBehtGF2Phb4BxeN2ytkTxh
1GEeroqocswEazxzeNAJh3KPPD7C61XY2H

+36,551,156.21

62fec42dd4370e0aeae88b3fe2a9970bb56a8d4bf0c...

2011-04-29 03:20:56

1MSUvGS9BEjpL35CKu7feF4HaPCXv2cht7

Bitcoin Address Summary for 1MSUvGS9BEjpL35CKu7feF4HaPCXv2cht7

$ 36,551,156.21

Home Charts Stats Wallet

# Bitcoin Address

**Summary**

| | |
|---|---|
| Address | 1MSUvGS9BEjpL35CKu7feF4HaPCXv2cht7 |
| Short Link | http://blockchain.info/fb/1msuv |
| Tools | Taint Analysis - Related Tags - Unspent Outputs |

**Transactions**

| | |
|---|---|
| No. Transactions | 2 |
| Total Received | 165,140 BTC |
| Final Balance | 0.00 BTC |

Request Payment | Donation Button

## Transactions

Filter

0121f30f11152b3df11904401e13b1b972a5408682...

2011-04-29 03:20:56

1B4JfdD4jGUWBehtGF2Phb4BxeN2ytkTxh
1GEeroqocswEazxzeNAJh3KPPD7C61XY2H

-165,140 BTC

62fec42dd4370e0aeae88b3fe2a9970bb56a8d4bf0c...

2011-04-29 03:20:56

1MSUvGS9BEjpL35CKu7feF4HaPCXv2cht7

185.140 BTC

# Bitcoin Address

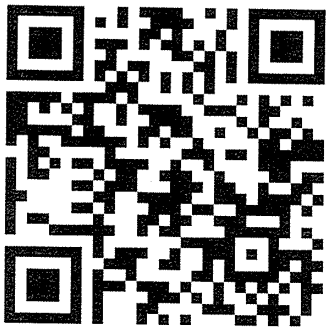
**Summary**

| | |
|---|---|
| Address | 12hRmmSda9qSSEH656zBaKEbeisH6ZhdTm |
| Short Link | http://blockchain.info/fb/12hrmm |
| Tools | Taint Analysis - Related Tags - Unspent Outputs |

**Transactions**

| | |
|---|---|
| No. Transactions | 2 |
| Total Received | 334,587.42424242 BTC |
| Final Balance | 0.00 BTC |

Request Payment | Donation Button



## Transactions

Filter

ddb352955903db83f76edb85f2121c51859b2f41a3... 2011-08-27 02:29:26

1PWr5e1JjL8wy6uzKzb5d3pCxkNLYm5vt1
1JjtxXmbC95sgn5kE2Hm92axA7hcbDkRhK

-334.587 42424242 BTC

796187f76168cd0ca2fff6c3f967fe28242429cec320e... 2011-08-27 02:29:26

12hRmmSda9qSSEH656zBaKEbeisH6ZhdTm

Bitcoin Address Watched: 12hRmmSda9qSSEH656zBaKEbeisH6ZhdTm

Balance: 42424242 BTC

This is annexure H marked with the letter H referred to in the affirmation / statutory declaration of Craig Wright sworn/affirmed/declared before me at Sydney on the 4th day of November 2013

One page only
Page 1 of 2 pages

Nicholas Charles McDonald
Justice of the Peace Registration 105174

H

# Statutory Declaration

OATHS ACT 1900, NSW, EIGHTH SCHEDULE

I, Stephen D'Emilio, of Level 3, 2 Bligh Street, Sydney, in the State of New South Wales, Solicitor, do solemnly and sincerely declare that:

1. I am the solicitor acting for Mr Craig Wright and Hotwire Pre-emptive Intelligence Pty Ltd.

2. On 11 October 2013, Mr Wright came into my office and showed me his HTC mobile phone (**Wright mobile**).

3. On the screen of the Wright mobile, I viewed and verified the following Bitcoin wallet addresses:

   (i) 1JzzLXxuwn45S9HvBqAhkhWa3GhyG3zm64;

   (ii) 168Rc6wJdL4chWhEUQwyywi4sHub6erf2s;

   (iii) 1FeexV6bAHb8ybZjqQMjJrcCrHGW9sb6uF;

   (iv) 1933phfhK3ZgFQNLGSDXvqCn32k2buXY8a; and

   (v) 16cou7Ht6WjTzuFyDBnht9hmvXytg6XdVT (**Bitcoin wallet addresses**).

4. I viewed the Bitcoin wallet addresses by scrolling down the screen on the Wright mobile.

5. It appeared to me that if Mr Wright wanted to, he could control all of, and make transactions in, the Bitcoin wallet addresses.

6. I make this solemn declaration conscientiously believing the same to be true and by virtue of the provisions of the *Oaths Act 1900*.

Declared at Sydney on 11 October 2013

.....
Stephen D'Emilio

in the presence of an authorised witness, who states:

I, Adrian Fong, a solicitor certify the following matters concerning the making of this statutory declaration by the person who made it:

1

(i) I saw the face of the person;

(ii) I have known the person for at least 12 months.

Adrian Fong

11 October 2013

## Craig S Wright

**From:** BAA Program Support Office <dhsbaa@reisys.com>
**Sent:** Wednesday, 2 March 2011 8:56 AM
**To:** Craig S. Wright; Craig S. Wright; Craig S. Wright
**Subject:** BAA BAA 11-02-TTA 09-0049-WP Upload Received

Your upload has been received electronically at the DHS BAA Support Office.

BAA 11-02 Proposal #: BAA 11-02-TTA 09-0049-WP
Proposal Title: Risk Quantification
Company Name: W&K INFO DEFENSE RESEARCH LLC

White Paper Uploaded on: 03/01/11 04:55 PM EST
File Name: BAA 11-02-TTA 09-0049-WP Risk Quantification.pdf
File Type: Portable Document Format
File Size: 357845 bytes

Uploaded by: Craig S. Wright

This is your official confirmation of receipt. Please save this email for your records, as no other receipt will be provided.

Thank you for your participation in the DHS BAA Program.

Please login to the portal at https://baa2.st.dhs.gov/portal/BAA/

If you have any questions, please contact DHS Technical Support at dhsbaa@reisys.com or call (703) 480-7676

Sincerely,
DHS BAA Program Support

This is the annexure marked with the letter "1" referred to in the Affidavit / ~~Affirmation / Statutory Declaration of~~ Craig Steven Wright
~~sworn/affirmed/declared~~ before me at [illegible] on the 4th day of November 2013
~~One page only~~ Page 1 of 4 pages
NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174

**Craig S Wright**

**From:** BAA Program Support Office <dhsbaa@reisys.com>
**Sent:** Wednesday, 2 March 2011 9:00 AM
**To:** Craig S. Wright; Craig S. Wright; Craig S. Wright
**Subject:** BAA BAA 11-02-TTA 01-0127-WP Upload Received

Your upload has been received electronically at the DHS BAA Support Office.

BAA 11-02 Proposal #: BAA 11-02-TTA 01-0127-WP
Proposal Title: Software Assurance through Economic Measures
Company Name: W&K INFO DEFENSE RESEARCH LLC

White Paper Uploaded on: 03/01/11 04:59 PM EST
File Name: BAA 11-02-TTA 01-0127-WP Software Assurance through Economic Measures.pdf
File Type: Portable Document Format
File Size: 290708 bytes

Uploaded by: Craig S. Wright

This is your official confirmation of receipt. Please save this email for your records, as no other receipt will be provided.

Thank you for your participation in the DHS BAA Program.

Please login to the portal at https://baa2.st.dhs.gov/portal/BAA/

If you have any questions, please contact DHS Technical Support at dhsbaa@reisys.com or call (703) 480-7676

Sincerely,
DHS BAA Program Support



## Craig S Wright

**From:** BAA Program Support Office <dhsbaa@reisys.com>
**Sent:** Wednesday, 2 March 2011 10:46 AM
**To:** Wright, Craig S. ; Wright, Craig S. ; Wright, Craig S.
**Subject:** Submission confirmation of your DHS BAA Program Proposal # BAA 11-02-TTA 01-0127-WP

Your proposal has been received electronically at the DHS Program Support Office.

BAA 11-02 White Paper Proposal #: BAA 11-02-TTA 01-0127-WP
Proposal Title: Software Assurance through Economic Measures
Company Name: W&K INFO DEFENSE RESEARCH LLC

Proposal Details:
Cover Sheet A completed on: 02/16/11 02:33 AM EST
Cover Sheet B completed on: 02/16/11 12:50 AM EST
White Paper Upload completed on: 03/01/11 04:59 PM EST
File Name: BAA 11-02-TTA 01-0127-WP Software Assurance through Economic Measures.pdf
File Type: Portable Document Format
File Size: 283 KB bytes

Submitted electronically by: Wright, Craig S.

This is your official confirmation of receipt. Please save this email for your records, as no other receipt will be provided.

Thank you for your participation in the DHS BAA Program.

Please login to the portal at https://baa2.st.dhs.gov/portal/BAA/

If you have any questions, please contact DHS Technical Support at dhsbaa@reisys.com or call (703) 480-7676

Sincerely,
DHS BAA Program Support

**Craig S Wright**

**From:** BAA Program Support Office <dhsbaa@reisys.com>
**Sent:** Wednesday, 2 March 2011 10:53 AM
**To:** Wright, Craig S. ; Wright, Craig S. ; Wright, Craig S.
**Subject:** Submission confirmation of your DHS BAA Program Proposal # BAA 11-02-TTA 09-0049-WP

Your proposal has been received electronically at the DHS Program Support Office.

BAA 11-02 White Paper Proposal #: BAA 11-02-TTA 09-0049-WP
Proposal Title: Risk Quantification
Company Name: W&K INFO DEFENSE RESEARCH LLC

Proposal Details:
Cover Sheet A completed on: 02/16/11 02:30 AM EST
Cover Sheet B completed on: 02/16/11 01:22 AM EST
White Paper Upload completed on: 03/01/11 04:55 PM EST
File Name: BAA 11-02-TTA 09-0049-WP Risk Quantification.pdf
File Type: Portable Document Format
File Size: 349 KB bytes

Submitted electronically by: Wright, Craig S.

This is your official confirmation of receipt. Please save this email for your records, as no other receipt will be provided.

Thank you for your participation in the DHS BAA Program.

Please login to the portal at https://baa2.st.dhs.gov/portal/BAA/

If you have any questions, please contact DHS Technical Support at dhsbaa@reisys.com or call (703) 480-7676

Sincerely,
DHS BAA Program Support

Homeland Security

BAA Program

DHS Broad Agency Announcements (BAA) Program Portal



# Registration Form

**Please do not register yourself MORE THAN ONCE!**

Fill in your registration information below. If there are errors on the registration form, you will be asked to re-enter the Company PIN and user password. **(Note: For security reason, this page will expire after 20 minutes of inactivity.)**

Re(g)ister | Back

*** Required Information**

This is the annexure marked with the letter "J" referred to in the Affidavit / Affirmation / Statutory Declaration of Greg S WRIGHT sworn/affirmed/declared before me at Sydney on the 4th day of December 2013

One page only
Page 1 of 6 pages

NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174

**COMPANY INFORMATION**

| | | |
|---|---|---|
| *Company Name: | W&K INFO DEFENSE RESEARCH LLC | |
| TIN: | 274997114 | |
| *Address (Line 1): | 4371 Norhtlake Blvd #314 | |
| Address (Line 2): | | *E-mail us* if you need to modify the TIN. |
| *City: | Palm Beach | |
| State: | FL | |
| *ZIP+4: | 33410 - 6253 Need help for ZIP+4? | |
| *Phone: | 561-310-8801 | Company's Phone and Fax. Enter only numbers |
| Fax: | | |
| *CEO/President's E-mail: | dave@davekleiman.com | |
| DUNS + 4: | - What is DUNS? | 9-digit Data Universal Number System plus a 4-digit suffix given by parent concern |
| CAGE Code: | How do I get a CAGE? | |
| SIC: | What is a SIC? | |
| FICE: | What is a FICE? | |
| Company URL: | http://www.information-defense.com/ | Provide Full URL *(http://www.example.com)* |
| *Year of Company Founded: | 2011 | |
| *Company PIN: | •••••• Why do you need a PIN? | Should be all numeric; no blank spaces allowed. Length must be between 4-6 numbers. |
| *Confirm Company PIN: | •••••• | |

**COMPANY POINT OF CONTACT INFORMATION**

| | | |
|---|---|---|
| *Salutation: | Mr. | |
| *First Name: | Craig | |
| Middle Initial: | S | |
| *Last Name: | Wright | |
| *Title: | Lead Researcher | |
| *Phone: | 61 (417) 683 914 Ext: | Enter only numbers |
| Fax: | | |
| *E-mail Address: | craig.wright@information-defense.c | **Important!** Fill out carefully |
| *Confirm E-mail Address: | craig.wright@information-defense.c | Re-enter E-mail Address |

**USER INFORMATION**

☑ Check here if you are also the Company Point Of Contact. *(This will pre-populate your information.)*

| | |
|---|---|
| *Salutation: | Mr. |

| | | |
|---|---|---|
| *First Name: | Craig | |
| Middle Initial: | S | |
| *Last Name: | Wright | |
| *Title: | Lead Researcher | |
| *Phone: | 61 (417) 683 914 Ext: | Enter only numbers |
| Fax: | | |
| *E-mail Address: | craig.wright@information-defense.c | **Important!** Fill out carefully |
| *Confirm E-mail Address: | craig.wright@information-defense.c | Re-enter E-mail Address |
| *Username: | CraigWright | Only alphanumeric characters and underscores are allowed. Username must be at least 8 characters. |
| *Password: | •••••••••••••••••• | Your password must be at least 8 characters long and must have an upper case, a lower case, a number, and a special character. Your new password cannot repeat any of your 8 previous passwords. |
| *Confirm Password: | •••••••••••••••••• | |
| PIN Contact: | ☑ **Check here if you want to list yourself as a contact for Company's PIN.** | |
| | **Additional Authentication (used if you forget your password)** | |
| *Select your question: | Who is your favorite person? | You will be prompted with this question and a new password will be issued automatically if your answer matches the one you give here |
| *Answer to above question: | Myself | |

*** Required Information**

Re(g)ister Back

DHS Form 10025 (7/07)

- U.S. Department of Homeland Security
- Science & Technology
- S&T Directorate SBIR Website
- OSDBU
- SAFETY Act
- SECURE Program
- Contact Us

## Craig S Wright

**From:** Dave Kleiman <dave@davekleiman.com>
**Sent:** Wednesday, 16 February 2011 2:22 PM
**To:** craig.wright@Information-defense.com
**Cc:** lynn.wright@information-defense.com
**Subject:** RE: Registration - TTA1
**Attachments:** W&K Info Defense Research LLC - 08.pdf

**Importance:** High

Look over the attached real quickly.

Let me know if it is ok.

Or should the PoC be in the US?? I see a non US vendor on the list.

Pay special attention to "Additional Authentication"

Dave

-----Original Message-----
From: Craig S Wright [mailto:craig.wright@information-defense.com]
Sent: Tuesday, February 15, 2011 22:04
To: Dave Kleiman
Subject: RE: Registration - TTA1

51 Cowangarra Rd
Bagnoo, New South Wales, 2446
AU

The other is not any longer

-----Original Message-----
From: Dave Kleiman [mailto:dave@davekleiman.com]
Sent: Wednesday, 16 February 2011 1:08 PM
To: craig.wright@Information-defense.com; lynn.wright@information-defense.com
Subject: RE: Registration - TTA1

Are either of these your current address?

51 Cowangarra Rd
Bagnoo, New South Wales, 2446
AU

Level 19, 2 Market Street
Sydney, NSW 2000

AU

-----Original Message-----
From: Dave Kleiman
Sent: Tuesday, February 15, 2011 14:13
To: 'craig.wright@Information-defense.com'; 'lynn.wright@information-defense.com'
Subject: RE: Registration - TTA1

It is under vendor registration that it requested DUNS see:
https://www.fbo.gov/?s=main&mode=list&tab=register&subtab=step1

Dave

-----Original Message-----
From: Dave Kleiman
Sent: Tuesday, February 15, 2011 07:29
To: 'craig.wright@Information-defense.com'; 'lynn.wright@information-defense.com'
Subject: RE: Registration - TTA1
Importance: High

Last page of attached. Do you think I can list you as mgr or mgrm with a foreign address, or you think they would kick it back?

Dave

-----Original Message-----
From: Dave Kleiman
Sent: Tuesday, February 15, 2011 06:35
To: 'craig.wright@Information-defense.com'; lynn.wright@information-defense.com
Subject: RE: Registration - TTA1

Did you already create a username and password?

-----Original Message-----
From: Craig S Wright [mailto:craig.wright@information-defense.com]
Sent: Tuesday, February 15, 2011 04:48
To: Dave Kleiman; lynn.wright@information-defense.com
Subject: Registration - TTA1

The first is to do with the attached papers...

TTA 01
<https://baa2.st.dhs.gov/portal/action/processRequest.action?eurl=AAAAAAEytBoAAAEuKK8xRgAUQUVTL0NCQy9QS0NTNVBhZGRpbmcAgAAQABAAAQIDBAUGBwgJCgsMDQ4PAAAAYMUP8ssYOu8SxeEfopmq%2F3IzhM%2F3rhjRC7iE1fh3qm1MXOKybn1NrHVavYBx1eeYUN3%2F6NSLR8PelSRUj0y6vIcWkXCDFPvq9gwzP%2BL6NcP3DCcUZ%2FjCxvXo415tuR%2Bt1gAU7aqi30%2B%2FBa8MygMsXUmvQKEcJuQ%3D#0> - Software Assurance

White paper title Software assurance through economic measures

This also leads to the following one with:

TTA 14
<https://baa2.st.dhs.gov/portal/action/processRequest.action?eurl=AAAAAAEytBoAAAEuKK8xRgAUQUVTL0NCQy9QS0NTNVBhZGRpbmcAgAAQABAAAQIDBAUGBwgJCgsMDQ4PAAAAYMUP8ssYOu8SxeEfopmq%2F3IzhM%2F3rhjRC7iE1fh3qm1MXOKybn1NrHVavYBx1eeYUN3%2F6NSLR8PelSRUj0y6vIcWkXCDFPvq9gwzP%2BL6NcP3DCcUZ%2FjCxvXo415tuR%2Bt1gAU7aqi30%2B%2FBa8MygMsXUmvQKEcJuQ%3D#13> - Software Assurance MarketPlace (SWAMP)

White paper title Software derivative markets

And

Information Security risk markets

Greyfog (last email) should also come under TTA 05
<https://baa2.st.dhs.gov/portal/action/processRequest.action?eurl=AAAAAAEytBoAAAEuKK8xRgAUQUVTL0NCQy9QS0NTNVBhZGRpbmcAgAAQABAAAQIDBAUGBwgJCgsMDQ4PAAAAYMUP8ssYOu8SxeEfopmq%2F3IzhM%2F3rhjRC7iE1fh3qm1MXOKybn1NrHVavYBx1eeYUN3%2F6NSLR8PelSRUj0y6vIcWkXCDFPvq9gwzP%2BL6NcP3DCcUZ%2FjCxvXo415tuR%2Bt1gAU7aqi30%2B%2FBa8MygMsXUmvQKEcJuQ%3D#4> - Secure, Resilient Systems and Networks

...

Dr. Craig S Wright <http://gse-compliance.blogspot.com/> GSE-Malware, GSE-Compliance, LLM, & ...

Information Defense <http://www.information-defense.com/> Pty Ltd

Mobile: 0417 683 914

Description: Logo4

**Proposal White Paper** **(Type I)**

| | |
|---|---|
| **BAA number**, • | BAA 11-02-TTA 01-0127-WP |
| **Title of proposal;** | Software Assurance through Economic Measures |
| **Name of offeror** | W&K INFO DEFENSE RESEARCH LLC |
| Administrative Contact: | Dave Kleiman |
| Company Name: | W&K INFO DEFENSE RESEARCH LLC |
| Mailing Address (Line 1): | 4371 Norhtlake Blvd #314 |
| Mailing Address (Line 2): | |
| City: | Palm Beach |
| State & Zip Code: | FL 33410 - 6253 |
| Phone: | 5613108801 |
| Fax: | NA |
| TIN: | 274997114 |
| Technical Contact: | Craig Wright |
| Company Name: | W&K INFO DEFENSE RESEARCH LLC |
| Mailing Address (Line 1): | 4371 Norhtlake Blvd #314 |
| Mailing Address (Line 2): | |
| City: | Palm Beach |
| State & Zip Code: | FL 33410 - 6253 |
| Phone: | +61 2 4362 1512 |
| Fax: | NA |
| TIN: | 274997114 |

W&K INFO DEFENSE RESEARCH LLC is a Joint Venture Company between a US Vet. Owned Enterprise and an Australian Research Company.

| | |
|---|---|
| Amount Requested (in dollars): | $650000.00 |
| Duration: | 36 months |
| Requested Starting Date: | 07/04/2011 |
| Business Type: | Small Business |

**Executive Summary**

The deficiency of published quantitative data on software development and systems design has been a major ground for software engineering's failure to ascertain a proper scientific foundation. Past studies into coding practice have focused on software vendors. These developers have many distinctions from in-house projects that are not incorporated into the practices and do not align well with in-house corporate code development. In the past, building software was the only option but as the industry developed, the build vs. buy argument has swung back towards in-house development with the uptake of Internet connected systems. In general, this has been targeted towards specialized web databases and online systems with office systems and mainstream commercial applications becoming a 'buy' decision.

As companies move more and more to using the web and as 'cloud applications' become accepted, in-house development is becoming more common. This paper uses an empirical study of in-house software coding practices in Australian companies to both demonstrate that there is an economic limit to how far testing should proceed as well as noting the deficiencies in the existing approaches.

1.1 Related Work

Other studies of coding processes and reliability have been conducted over the last few decades. The majority of these have been based either on studies of large systems and mainframe based operations or have analyzed software vendors. In the few cases where coding practices within individual organization have been quantitatively analyzed, the organizations have been nearly always large telecommunications firms or have focused on SCADA and other critical system providers.

Whilst these results are extremely valuable, they fail to reflect the state of affairs within the vast majority of organizations. With far more small to medium businesses coupled with comparatively few large organizations with highly focused and dedicated large scale development teams (as can be found in any software vendor), an analysis of in-house practice is critical to both security and the economics of in-house coding.

As the Internet becomes all persuasive, internal coding functions are only likely to become more prevalent and hence more crucial to the security of the organization.

1.2 Our contribution

We intend to present an analysis using empirical studies to determine and model the cost of finding, testing and fixing software bugs. We model the discovery of bugs or vulnerabilities in using quantitative functions and calculate the defect rate per SLOC (source line of codes) using Bayesian calculations.

The end solution to the limited and sub-optimal markets that currently exist would be the creation of Hedge funds for software security. Sales in software security based derivatives could be created on forward contracts. One such solution is the issuing of paired contracts (such as

exist in short sales of stocks ). The first contract would be taken by a user and would pay a fixed amount if the software has suffered from any unmitigated vulnerabilities on the (forward) date specified in the contract. The paired contract would cover the vendor. If the vendor creates software without flaws (or at least mitigates all easily determinable flaws prior to the inception of the contract) the contract pays them the same amount as the first contract.

This is in effect a 'bet' that the software will perform effectively. If a bug is discovered, the user is paid a predetermined amount. This amount can be determined by the user to cover the expected costs of patching and any consequential damages (if so desired). This allows the user to select their own risk position by purchasing more or less risk as suits both the risk tolerance and the nature of the user's systems.

Such a derivative (if an open market is allowed to exist) would indicate the consensus opinion as to the security of the software and the reputation of the vendor. Such an instrument would allow software vendors and users to hedge the risks faced by undiscovered software vulnerabilities. These instruments would also be in the interest of the software vendor's investors as the ability to manage risk in advance would allow for forward financial planning and limit the negative impact that vulnerability discovery has on the quoted prices of a vendors capital.

This project will model the security of software coding practices in a manner that will lead to fewer economic externalities

**Utility to Department of Homeland Security**

The game theoretic approach to this can be modeled looking at the incentives of the business and programming functions in the organization. Programmers are optimists. As Brooks noted, "the first assumption that underlies the scheduling of systems programming is that all will go well". Testing is rarely considered by the normal programmer as this would imply failure. However, the human inability to create perfection leads to the introductions of flaws at each stage of development.

**Technical Approach**

Just as car dealers buff the exterior and detail the upholstery of a used car, neglecting the work that should be done on the engine, software vendors add features. Most users are unlikely to use even a small fraction of these features, yet they buy the product that offers more features over the more secure product with fewer features. The issue here is that users buy the features over security. This is a less expensive option for the vendor to implement and provide.

The creation of a security and risk derivative should change this. The user would have an upfront estimate of the costs and this could be forced back to the software vendor. Where the derivative costs more than testing, the vendor would conduct more in-depth testing and reduce the levels of bugs. This would most likely lead to product differentiation (as occurred in the past with Windows 95/Windows NT). Those businesses who wish to pay for security could receive it. Those wanting features would get what they asked for.



It is argued that software developers characteristically do not correct all the security vulnerabilities and that known ones remain in the product after release. Whether this is due to a lack of resources or other reasons, this is unlikely to be the norm and would be rectified by the market. The cost of vendors in share price and reputational losses exceed the perceived gains from technical reasons where the fix might break existing applications. The application is already broken in the instance of a security vulnerability.

Users could still run older versions of software and have few, if any, bugs. The issue is that they would also gain no new features. It is clear that users want features. They could also choose to use only secure software, but the costs of doing so far outweigh the benefits and do not provide a guarantee against the security of a system being compromised. As such, the enforced legislation of security standards against software vendors is detrimental. A better approach would be to allow an open market based system where vendors can operate in reputational and derivative markets.

At the end of any analysis, security is a risk function and what is most important is not the creation of perfectly security systems, but the correct allocation of scarce resources. Systems need to be created that allow the end user to determine their own acceptable level of risk based on good information.

The goal of this research project is to create a series of quantitative models for information security that can be used to create a software security derivative and insurance market. Mathematical modeling techniques that can be used to model and predict information security risk will be developed using a combination of techniques including:

- Economic theory, and Econometrics
- Quantitative financial modeling,
- Behavioral Economics,
- Algorithmic game theory and
- Statistical hazard/survival models.

The models will account for heteroscedastic confounding variables and include appropriate transforms such that variance heterogeneity is assured in non-normal distributions. Process modeling for integrated Poisson continuous-time process for risk through hazard will be developed using a combination of:

- Business financial data (company accountancy and other records),
- Anti-Virus Industry data
- Legal databases for tortuous and regulatory costs and
- Insurance datasets.

**<u>This work and research follows and continues that published as:</u>**

> Wright, Craig S. and Zia, Tanveer A. (2010) T*he Economics of Developing Security Embedded Software*, Proceedings of the 8th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 30th November 2010

Charles Sturt University

http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1101&context=ism

and

Wright, Craig S. (2010) *Software, Vendors and Reputation: an analysis of the dilemma in creating secure software*, Proceedings of InTrust 2010 The Second International Conference on Trusted Systems 13th – 15th December 2010 Beijing, P. R. China

Charles Sturt University

and (forthcoming)

Wright, Craig S. and Zia, Tanveer A (2011) *A Quantitative Analysis into the Economics of Testing Software Bugs*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011

Wright, Craig S. and Zia, Tanveer A (2011) *A Rationally Opting for the Insecure Alternative: Negative Externalities and the Selection of Security Controls*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011

**Personnel and Performer Qualifications and Experience**

**Craig S Wright (Full CV too long and is available in request)**

Over the years Craig has personally conducted and managed in excess of 1,600 IT security related engagements for more than 180 Australian and international organizations in both the private and government sectors. As a strong believer in life-long learning, Craig has qualifications in Law, IT, Mathematics and Business. However, his driving focus is research and development in the security and risk arena. He is the first person to have obtained multiple GSE certifications (Malware and Compliance) Craig designed the architecture for the world's first online casino (Lasseter's Online) in the Northern Territory; as well he has, in the past, designed and managed the implementation of many of the systems that protect the Australian Stock Exchange. To add to these accomplishments he has authored IT security related books and articles as well as designed a new university program for Charles Sturt University in New South Wales, Australia which will offer a Master in Digital Forensics. This program commenced in 2010 and be offered as an on campus and distance education program.

**Dave Kleiman** (http://en.wikipedia.org/wiki/Dave_Kleiman)

Dave Kleiman is a noted Forensic Computer Investigator, an author/coauthor of multiple books and a noted speaker at security related events

**Bob Radvanovsky**, CIFI, CISM, REM, CIPS, Infracritical, Inc.
Principle, SCADA expert and Author
(chapter author) of "Corporate Hacking and Technology-driven Crime: Social Dynamics and Implication", ISBN 1616928050 and 9781616928056, Information Science Publishing, July 2010.

URL: http://www.amazon.com/Corporate-Hacking-Technology-driven-Crime-Implications/dp/1616928050

"Challenges Faced by the SCADASEC Mailing List", Protecting Canada's Critical Infrastructure 2010 Control Systems Security Workshop, sponsored by Royal Canadian Mounted Police (Ontario Technological Crime), Public Safety Canada and Emergency Management Ontario (Critical Infrastructure Assurance Program), Wednesday April 14, 2010 and Thursday, April 15, 2010.
URL: http://www.infracritical.com/papers/scadasec-2010-review.zip
Author of "Critical Infrastructure: Homeland Security and Emergency Preparedness", Second Edition, ISBN 1420095277 and 9781420095272, Taylor & Francis CRC Press, December 2009.
URL: http://www.amazon.co.uk/Critical-Infrastructure-Homeland-Emergency-Preparedness/dp/1420095277
Contributor (introduction speaker) of "The Year in Homeland Security", 2008/2009 Edition (Charles Oldham, editor director), Faircount Media Group.
URL: http://viewer.zmags.com/publication/d1408139#/d1408139/12
Author (co-author) of "Transportation Systems Security", ISBN 1420063782 and 9781420063783, Taylor and Francis CRC Press, May 2008.
URL: http://www.amazon.com/Transportation-Systems-Security-Allan-McDougall/dp/1420063782

**Commercialization Capabilities and Plan**

The principles are experienced researchers and businessmen in the realm of Information Security. The research will be conducted in conjunction with Charles Sturt University and will follow the standard commercialization processes of the University (these processes are available online). Further, this project will create a large body of public and academic knowledge and scientific research that could also be used by other companies and Universities in the creation of further models and structures that will lead to the securing of more systems again.

**Costs, Work, and Schedule**

| | |
|---|---|
| Amount Requested (in dollars): | $650,000.00 |
| Duration: | 36 months |

The funding request will provide full scholarships and positions for three (3) PhD candidates to aide in the research and investigation of software security issues and solution, the creation of economic models and the publication of an expected 20-30 papers in this field.

The period is set to three years which includes the completion of the PhD projects and the creation of the market, insurance and derivative models.

- PhD Funding $240,000
- Supervision $180,000
- Survey and data Analysis $230,000

| | |
|---|---|
| **BAA Number:** BAA 11-02-TTA 01-0127-WP<br>**Offeror Name:** W&K INFO DEFENSE RESEARCH LLC<br>**Title** Software Assurance through Economic Measures<br>**Date:** 07/04/2010 | |
| N/A | **Operational Capability:**<br>The project will analyze a sample of at least 1,000 coding projects using existing static analysis tools, manual code review and related techniques. Where these methods are lacking, proposals and methods to integrate existing methods and to fill the gaps left will be created. |
| **Proposed Technical Approach:**<br>This project will address and provide measures and The analysis will measure the following coding errors:<br>• Format string errors<br>• Integer Overflows<br>• Buffer overruns<br>• SQL Injection<br>• Cross-Site scripting<br>• Race Conditions<br>• Command Injection.<br>Several published papers have been released (forthcoming include)<br><br>Wright, Craig S. and Zia, Tanveer A (2011) *A Quantitative Analysis into the Economics of Testing Software Bugs*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011<br><br>Wright, Craig S. and Zia, Tanveer A (2011) *A Rationally Opting for the Insecure Alternative: Negative Externalities and the Selection of Security Controls*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011 | **Schedule, Cost, Deliverables, & Contact Info:**<br>Provide any milestone decision points that will be required. Describe period of performance and total costs. Include the base performance period cost and length, and estimates of cost and lengths of possible option.<br>**Deliverables:**<br>20-30 published papers<br>3 PhD Thesis' in the field<br>A commercial model for software derivatives and insurance markets<br><br>A means to measure and predict the following coding errors is being developed<br>Format string errors<br>Integer Overflows<br>Buffer overruns<br>SQL Injection<br>Cross-Site scripting<br>Race Conditions<br>Command Injection.<br><br>**Corporate Information:**<br>Dave Kleiman<br>W&K INFO DEFENSE RESEARCH LLC<br>4371 Norhtlake Blvd #314<br>Palm Beach<br>FL 33410 - 6253<br><br>Phone: 5613108801<br>Email: dave@davekleiman.com |

Authorized Representative: Craig Wright

Signature:

| | |
|---|---|
| **Proposal White Paper** | **(Type I)** |
| **BAA number**, • | BAA 11-02-TTA 09-0049-WP |
| **Title of proposal;** | Risk Quantification |
| **Name of offeror** | W&K INFO DEFENSE RESEARCH LLC |
| Administrative Contact: | Dave Kleiman |
| Company Name: | W&K INFO DEFENSE RESEARCH LLC |
| Mailing Address (Line 1): | 4371 Norhtlake Blvd #314 |
| Mailing Address (Line 2): | |
| City: | Palm Beach |
| State & Zip Code: | FL 33410 - 6253 |
| Phone: | 5613108801 |
| Fax: | NA |
| TIN: | 274997114 |
| Technical Contact: | Craig Wright |
| Company Name: | W&K INFO DEFENSE RESEARCH LLC |
| Mailing Address (Line 1): | 4371 Norhtlake Blvd #314 |
| Mailing Address (Line 2): | |
| City: | Palm Beach |
| State & Zip Code: | FL 33410 - 6253 |
| Phone: | +61 2 4362 1512 |
| Fax: | NA |
| TIN: | 274997114 |

W&K INFO DEFENSE RESEARCH LLC is a Joint Venture Company between a US Vet. Owned Enterprise and a Australian Research Company.

| | |
|---|---|
| Amount Requested (in dollars): | $2,200,000.00 |
| Duration: | 36 months |
| Requested Starting Date: | 07/04/2011 |
| Business Type: | Small Business |

**Executive Summary**

Using empirical evidence, this research aims to investigate and quantify the root cause of security flaws that act as a source of system compromise. Research into the effects of poor system design, market based risk solutions based on derivative instruments and the impact of common system misconfigurations will be incorporated into multivariate survival models. This research incorporates the economic impact of various decisions as a means of determining the optimal distribution of costs and liability when applied to information security and in particular when assigning costs in computer system security and reliability engineering.

The objective of this research is to produce an innovative modelling architecture designed around information systems security and risk based reliability and survivability analysis. The objectives of the research are:

(1) To address the critical limitations (Jeanblanc & Valchev, 2005) that are associated with reliability engineering in regards to computer systems. This will be completed with competing risks analysis and multivariate survival analysis coupled with a game theoretic approach. Data collected from an analysis of systems in the field will be used to test assumptions. These assumptions (Marti, 2008) include:
    a. constant and homogenous failure rates,
    b. binary failure and univariate reliability,
    c. censoring of failure data, and
    d. independent failures.

(2) To produce a methodology for the creation and testing of hazard and survival models for information systems. This will become a risk based quantitative approach to reliability and survivability engineering.

(3) To incorporate methods that represent the effects of misaligned incentives and their consequence to security controls.

To do this, it is necessary to recognise that information security is a risk function (Anderson, Longley & Kwok, 1994). Paying for too much security can be more damaging in economic terms than not buying enough. This leads to decisions about where the optimal expenditure on damage prevention should lie. This research will investigate who should be responsible for the security failures that are affecting the economy and society and how can this be maximized in order to minimize negative externalities (Cohen, 1976). The conclusions will be presented using an empirical study of software hazard rates and audit failures along with the question of how to enforce liability in a global economy.

The research is intended to address some of the economic issues that are arising due to an inability of assign risk correctly, a failure to measure risk as well as looking at the misalignment of information systems audit and the compliance regime. The externalities that restrict the development of secure software and how the failure of the end user to apply controls makes it less probable that a software vendor will enforce stricter programming controls with failures in the audit and measurement processes are addressed. This includes a look at the misalignment of audit to security. This misalignment is demonstrated to result from the drawing of funds from security in order to provide compliance with little true economic gain (Wright, 2010).

The introduction of Game Theory and Behavioural Economics (Anderson, 2001; Anderson, & Moore, 2006; Varian, 2004) have created a foundation for the rationalisation of information security processes which lead to improved allocation of economic resources. The optimal distribution of economic resources across risk allocations in information system can only lead to

a combination of more secure systems for a lower overall cost. This research will incorporate the game theoretic multi-player decision problem. Agents in the model will be deemed to be rational with well-defined preferences, include the ability to reason strategically using their knowledge and belief of other players and to act according to a combination of both economic "*first thought*" and deep strategic thinking (Nissan, et. al., 2007). Solutions to these models will be sought through a combination of the following game devices:

- Equilibrium: evolutive (steady state) games
- Heterogeneous sequential games
- Rationalisability: deductive reasoning

The models will detail the existence of strictly dominating games where these exist in information security practices and propose methods to improve these models. Existing information security practices in existing organisations will be classified into the following game types:

- Non-cooperative vs. cooperative game
- Strategic vs. extensive game
- Perfect vs. imperfect information

Bounded rationality, behavioural game aspects and other feedback effects will be investigated (Nissan, et. al., 2007). Social capital based on fairness and reciprocity will be defined as it applies to the economically efficient application of risk processes associated with Information systems. Contract Theory will be used to explain the creation of agreements and "*contracts*" in the presence of information asymmetry. This is approached through the combination of adverse selection, moral hazards and the "*signalling game*". In this, adverse selection is defined as the "*Principal not having been informed of the other agent's private information ex-ante*" such as in George Akerlof's "*Market for lemons*" (1970). This application of game theory has been asserted to explain many aspects of the software industries predisposition to create insecure software (Anderson, 2001). Arora, Telang and Xu (2004) asserted that a market-based mechanism for software vulnerabilities would necessarily underperform a CERT-type mechanism. The market that they used was a game theoretic *pricing game*. In the model reported, the players in the market do not report their prices[1]. These players use a model where information is distributed simultaneously to the client of the player and the vendor. The CERT model was touted as being the most favourable solution. The research will demonstrate that the examined "*market*" model is in itself sub-optimal. It both creates incentives to leak information without proper safeguards and creates vulnerability black-markets that rely on waiting until a patch was publically released and only then releasing the patch to the public. This ignores many externalities and assumes the only control is a patch in place of other alternative compensating controls. It is to be demonstrated that there are flaws with this approach that can be solved through the creation of a security and risk derivative market for software. The user would have an upfront estimate of the costs and this could be forced back to the software vendor. Where the derivative costs more than testing, the vendor would conduct more in-depth testing and reduce the levels of bugs (Bacon et. al. 2009).

### 1.2 Our contribution and Technical Approach

We intend to present an analysis using empirical studies to determine and model the cost of finding, testing and fixing security vulnerabilities. The goal of this research project is to create a series of quantitative models for information security. Mathematical modelling techniques that

[1] E.g., iDefense Ltd. and other similar providers have a semi-closed market with limited information exchange.

can be used to model and predict information security risk will be developed using a combination of techniques including:

- Economic theory, and Econometrics
- Quantitative financial modelling,
- Behavioural Economics,
- Algorithmic game theory and
- Statistical hazard/survival models.

The models will account for heteroscedastic confounding variables and include appropriate transforms such that variance heterogeneity is assured in non-normal distributions. Process modelling for integrated Poisson continuous-time process for risk through hazard will be developed using a combination of:

- Business financial data (company accountancy and other records),
- Anti-Virus Industry data
- Legal databases for tortuous and regulatory costs and
- Insurance datasets.

This data will be coupled with hazard models created and validated using Honeynets (e.g. Project Honeynet), reporting sites such as the Internet Storm Centre and iDefence. The combination of this information will provide the framework for a truly quantitative security risk framework[2]. At present, the DShield storm centre receives logging from over 600,000 organisations. This represents a larger quantity of data than is used for actuarial data in the home insurance industry. The problem being that this information is not collated or analysed in any quantitatively sound manner. This research will model survival times for types of applications using the body of research into quantitative code analysis for risk. The research will create a series of models (such as those used within mechanical engineering, material science etc) for Information Risk.

Some of the methods that are planned testing in the creation of the risk framework will include:

- Random forest clustering,
- K-means analysis,
- Other classification algorithms, and
- Network associative maps in text analysis forensic work.

The correlation of reference data (such as IP and functional analysis data) between C&C (Command and Control) systems used in "*botnets*" is one aspect of this research. Starting from the outside (the cloud and perimeter) and working inwards to the network, the risk model would start by assessing external threats and move into internal threat sources, becoming gradually become more and more granular as one moves from network to individual hosts and finally to people (user behaviour (Varian, 2004)) and application modelling (Guo, Jarrow, & Zeng, 2005). The eventual result will be the creation of a model that can incorporate the type of organisation, size, location, application, systems used, and the user awareness levels to create a truly quantitative risk model. This would be reported with SE (standard error) and confidence level rather than a point estimate. Code to import data from hosts and networks, using raw "*pcap traces*"[3] will be developed such that system statistics and other data can be collated into a standardised format. This code will be developed in "R" and "C++". This will enable the

[2] Support has been sought and received from SANS (including DShield), CIS (Centre for Internet Security) and the Honeynet project.
[3] Pcap is a packet capture standard supported by both open source and commercial network capture equipment.

creation and release of actuarial threat risk models that incorporate heterogeneous tendencies in variance across multidimensional determinants while maintaining parsimony. I foresee a combination of Heteroscedastic predictors (GARCH/ARIMA etc) coupled with non-parametric survival models. I expect that this will result in a model where the underlying hazard rate (rather than survival time) is a function of the independent variables (covariates). Cox's Proportional Hazard Model with Time-Dependent Covariates would be a starting point, going to non-parametric methods if necessary. The end goal will be to create a framework and possibly a program that can assess data stream based on a number of dependant variables (Threat models, system survival etc) and covariates and return a quantified risk forecast and standard error.

**Utility to Department of Homeland Security**

When a system fails, it often can fail in numerous ways with several causes for the failure (Crowder 2001). Censored observation management can be considered the principal factor influencing survival analysis. Survival analysis and has developed rigorous procedures and methods effective for the treatment of censored data based on probability theory, asymptotic counting and stochastic process as well as the Martingale central limit theorem. References to the univariate analysis of survival is found in Cox (1972), Cox and Oakes (1984), Fleming and Harrington (1991), Andersen et al (1993), Kalbfleisch and Prentice (1980, 2002), Klein and Moeschberger (2003), Ibrahim et al. (2005), Lawless (1982, 2003), Ma and Krings (2008).

Modeling risk allows it to be measured and controlled.

**<u>This work and research follows and continues:</u>**

Wright, Craig S. and Zia, Tanveer A. (2010) T*he Economics of Developing Security Embedded Software*, Proceedings of the 8th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 30th November 2010

Charles Sturt University

http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1101&context=ism

and (forthcoming)

Wright, Craig S. and Zia, Tanveer A (2011) *A Quantitative Analysis into the Economics of Testing Software Bugs*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011

Wright, Craig S. and Zia, Tanveer A (2011) *A Rationally Opting for the Insecure Alternative: Negative Externalities and the Selection of Security Controls*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011

**Personnel and Performer Qualifications and Experience**

**Craig S Wright (Full CV too long and is available in request)**

Over the years Craig has personally conducted and managed in excess of 1,600 IT security related engagements for more than 180 Australian and international organizations in both the private and government sectors. As a strong believer in life-long learning, Craig has qualifications in Law, IT, Mathematics and Business. However, his driving focus is research and development in the security and risk arena. He is the first person to have obtained multiple GSE certifications (Malware and Compliance) Craig designed the architecture for the world's first online casino (Lasseter's Online) in the Northern Territory; as well he has, in the past, designed and managed the implementation of many of the systems that protect the Australian Stock Exchange. To add to these accomplishments he has authored IT security related books and articles as well as designed a new university program for Charles Sturt University in

New South Wales, Australia which will offer a Master in Digital Forensics. This program commenced in 2010 and be offered as an on campus and distance education program.

**Dave Kleiman** (http://en.wikipedia.org/wiki/Dave_Kleiman)

Dave Kleiman is a noted Forensic Computer Investigator, an author/coauthor of multiple books and a noted speaker at security related events

**Bob Radvanovsky**, CIFI, CISM, REM, CIPS, Infracritical, Inc.

Principle, SCADA expert and Author

URL: http://www.amazon.com/Corporate-Hacking-Technology-driven-Crime-Implications/dp/1616928050

URL: http://www.infracritical.com/papers/scadasec-2010-review.zip

URL: http://www.amazon.co.uk/Critical-Infrastructure-Homeland-Emergency-Preparedness/dp/1420095277

URL: http://viewer.zmags.com/publication/d1408139#/d1408139/12

URL: http://www.amazon.com/Transportation-Systems-Security-Allan-McDougall/dp/1420063782

**Commercialization Capabilities and Plan**

The principles are experienced researchers and businessmen in the realm of Information Security. The research will be conducted in conjunction with Charles Sturt University and will follow the standard commercialization processes of the University (these processes are available online). Further, this project will create a large body of public and academic knowledge and scientific research that could also be used by other companies and Universities in the creation of further models and structures that will lead to the securing of more systems again.

**Costs, Work, and Schedule**

| | |
|---|---|
| Amount Requested (in dollars): | $2,200,000.00 |
| Duration: | 36 months |

The funding request will provide full scholarships and positions for three (3) PhD candidates to aide in the research and investigation of software security issues and solution, the creation of economic models and the publication of an expected 20-30 papers in this field.

The period is set to three years which includes the completion of the PhD projects and the creation of the market, insurance and derivative models.

- PhD Funding $480,000
- Supervision $350,000
- Survey and data Analysis $230,000
- Research Fellowships (2) $260,000
- Administration $120,000
- Costs (Computational Systems) $660,000
- Support Costs (Coding) $300,000

| | |
|---|---|
| **BAA Number:** BAA 11-02-TTA 01-0127-WP<br>**Offeror Name:** W&K INFO DEFENSE RESEARCH LLC<br>**Title** Risk Quantification<br>**Date:** 07/04/2010 | |
| N/A | **Operational Capability:**<br>The research is intended to address some of the economic issues that are arising due to an inability of assign risk correctly, a failure to measure risk as well as looking at the misalignment of information systems audit and the compliance regime. The externalities that restrict the development of secure software and how the failure of the end user to apply controls makes it less probable that a software vendor will enforce stricter programming controls with failures in the audit and measurement processes are addressed. This includes a look at the misalignment of audit to security. This misalignment is demonstrated to result from the drawing of funds from security in order to provide compliance with little true economic gain (Wright, 2010). |

**Proposed Technical Approach:**

The objective of this research is to produce an innovative modeling architecture designed around information systems security and risk based reliability and survivability analysis. The objectives of the research are:

(1) To address the critical limitations (Jeanblanc & Valchev, 2005) that are associated with reliability engineering in regards to computer systems. This will be completed with competing risks analysis and multivariate survival analysis coupled with a game theoretic approach. Data collected from an analysis of systems in the field will be used to test assumptions. These assumptions (Marti, 2008) include:

a. constant and homogenous failure rates,

b. binary failure and univariate reliability,

c. censoring of failure data, and

d. independent failures.

(2) To produce a methodology for the creation and testing of hazard and survival models for information systems. This will become a risk based quantitative approach to reliability and survivability engineering.

(3) To incorporate methods that represent the effects of misaligned incentives and their consequence to security controls.

**Schedule, Cost, Deliverables, & Contact Info:**

**Deliverables:**

30-40 published papers

3 PhD Thesis' in the field

A commercial model for modeling information risk

Several published papers have been released (forthcoming include)

Wright, Craig S. and Zia, Tanveer A (2011) A Quantitative Analysis into the Economics of Testing Software Bugs, Proceedings of CISIS 2011 June 8-10th, 2011

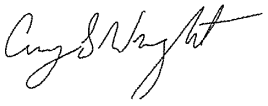
Wright, Craig S. and Zia, Tanveer A (2011) A Rationally Opting for the Insecure Alternative: Negative Externalities and the Selection of Security Controls, Proceedings of CISIS 2011, 2011

**Corporate Information:**

Dave Kleiman
W&K INFO DEFENSE RESEARCH LLC
4371 Norhtlake Blvd #314
Palm Beach
FL 33410 - 6253
Phone: 5613108801
Email: dave@davekleiman.com

Authorized Representative: Craig Wright

Signature:



**Proposal White Paper** **(Type I)**

| | |
|---|---|
| **BAA number**, • | BAA 11-02-TTA 14-0025-WP |
| **Title of proposal;** | Software Derivative Markets & Information Security Risk |
| **Name of offeror** | W&K INFO DEFENSE RESEARCH LLC |
| Administrative Contact: | Dave Kleiman |
| Company Name: | W&K INFO DEFENSE RESEARCH LLC |
| Mailing Address (Line 1): | 4371 Norhtlake Blvd #314 |
| Mailing Address (Line 2): | |
| City: | Palm Beach |
| State & Zip Code: | FL 33410 - 6253 |
| Phone: | 5613108801 |
| Fax: | NA |
| TIN: | 274997114 |
| Technical Contact: | Craig Wright |
| Company Name: | W&K INFO DEFENSE RESEARCH LLC |
| Mailing Address (Line 1): | 4371 Norhtlake Blvd #314 |
| Mailing Address (Line 2): | |
| City: | Palm Beach |
| State & Zip Code: | FL 33410 - 6253 |
| Phone: | +61 2 4362 1512 |
| Fax: | NA |
| TIN: | 274997114 |

W&K INFO DEFENSE RESEARCH LLC is a Joint Venture Company between a US Vet. Owned Enterprise and a Australian Research Company.

| | |
|---|---|
| Amount Requested (in dollars): | $1,200,000.00 |
| Duration: | 36 months |
| Requested Starting Date: | 07/04/2011 |
| Business Type: | Small Business |

**Executive Summary**

This project will develop the optimal derivative and risk strategy for software markets. A game theoretic approach to this will be modeled looking at the incentives of the business and programming functions in the organization. Programmers, as optimists (Brooks) hold, "the first assumption that underlies the scheduling of systems programming is that all will go well". Testing is rarely considered by the normal programmer as this would imply failure. However, the human inability to create perfection leads to the introductions of flaws at each stage of development. This project will deliver frameworks designed to optimize the software development process and to sell the risk using a derivative market place that reflects this risk. The end goal is to remove externalities from the costs of software and incorporate the cost of bad software design into the final cost to the consumer.

The deficiency of published quantitative data on software development and systems design has been a major ground for software engineering's failure to ascertain a proper scientific foundation. Past studies into coding practice have focused on software vendors. These developers have many distinctions from in-house projects that are not incorporated into the practices and do not align well with in-house corporate code development. In the past, building software was the only option but as the industry developed, the build vs. buy argument has swung back towards in-house development with the uptake of Internet connected systems. In general, this has been targeted towards specialized web databases and online systems with office systems and mainstream commercial applications becoming a 'buy' decision.

As companies move more and more to using the web and as 'cloud applications' become accepted, in-house development is becoming more common. This paper uses an empirical study of in-house software coding practices in Australian companies to both demonstrate that there is an economic limit to how far testing should proceed as well as noting the deficiencies in the existing approaches.

**1.1 Related Work and our contributions**

This research will seek to demonstrate that a well-defined software risk derivative market would improve the information exchange for both the software user and vendor removing the oft touted imperfect information state that is said to belie the software industry. In this way, users could have a rational means of accurately judging software risks and costs and as such the vendor could optimally apply their time between delivering features and averting risk in a manner demanded by the end user. After all, it is of little value to increase the cost per unit of software by more than an equal compensating control.

Arora, Telang and Xu asserted that a market based mechanism for software vulnerabilities will necessarily underperform a CERT-type mechanism. The market that they used was a game theoretic pricing game. In the model reported, the players in the market do not report their prices. These players use a model where information is simultaneously distributed to the client of the player and the vendor. The CERT model was touted as being optimal. It relies on waiting until a patch was publically released and only then releasing the patch to the public. This ignores many externalities and assumes the only control is a patch in place of other alternative compensating controls.

Consequently, the examined "market" model is in itself sub-optimal. It both creates incentives to leak information without proper safeguards and creates vulnerability black-markets. As criminal groups and selected security vendors (such as Penetration testers and IDS vendors) have an incentive to gain information secretly , they have an incentive to pay more for unknown vulnerabilities in a closed market. This means that a seller to one of these parties has a



reputational incentive to earn more through not releasing information as the individual's reputation will be based on their ability to maintain secrecy.

"Vulnerability disclosure adversely and significantly affects the stock performance of a software vendor. We show that, on average, a software vendor loses around 0.63% of market value on the day of the vulnerability announcement. This translates to a dollar amount of $0.86 billion loss in market value. We also show that markets do not penalize a vendor any more if the vulnerability is discovered by a third party than by the vendor itself."

These results demonstrate that a vendor has an incentive to minimize the vulnerabilities found in their products. If an excessive number of vulnerabilities continue to impact a vendor, their market capitalization suffers as a consequence. This justification offers strong evidence that a vendor does not have an incentive to hide information (as third party vulnerability researchers cause an equal loss in capitalization). It has to be expected that any vulnerability known by the vendor will be uncovered. If the vendor fixes this flaw before release, the cost is minimized and at the limit approaches the cost of testing, (that is a zero incremental cost to that which would be expressed later).

If the vendor discovers a vulnerability in the software they produce, the result is a 'strongly dominated' motive to fix the bug. Hence, any remaining bugs are those that have not been uncovered by the vendor and which are less economical to find (through an increase in testing). It can thus be demonstrated that the vendor knows no more than the user at the point of software release as to the state of bugs in a product.

Testing is far less expensive earlier in the development cycle. Early in the process, the software developer has the greatest returns in testing and bug finding. As the development progresses, the returns are reduced as the process required and the costs associated with finding and correcting software vulnerabilities increases.

The utility is lowest when the software has been shipped to the user. At this point, fixing flaws is an expensive process for both the user and the vendor. This leaves the optimal solution to find as many bugs as possible as early in the development process as is feasible. This contrasts with the increasing costs of finding bugs. This leaves the optimal solution for the vendor based on the discovery of as many bugs as possible as early in the development process as is feasible (as a bug discovered early in the process can cost as much as 10x less than one discovered later) . It does not mean that all bugs or vulnerabilities will be found as the cost of finding additional vulnerabilities quickly exceeds the returns.

The market for lemons requires that the vendor knows the level of flaws better than the user. To many this may seem a common sense outcome, the vendor has access to source code, wrote the program and ran the development process. This is a flawed view as we have demonstrated as it is in the vendor's interest to mitigate vulnerabilities as early as possible. More importantly, the vendor is punished for bugs.

1.2 Our contribution

We intend to present an analysis using empirical studies to determine and model the cost of finding, testing and fixing software bugs. We model the discovery of bugs or vulnerabilities in using quantitative functions and calculate the defect rate per SLOC (source line of codes) using Bayesian calculations.

The end solution to the limited and sub-optimal markets that currently exist would be the creation of Hedge funds for software security. Sales in software security based derivatives could be created on forward contracts. One such solution is the issuing of paired contracts (such as exist in short sales of stocks ). The first contract would be taken by a user and would pay a fixed



amount if the software has suffered from any unmitigated vulnerabilities on the (forward) date specified in the contract. The paired contract would cover the vendor. If the vendor creates software without flaws (or at least mitigates all easily determinable flaws prior to the inception of the contract) the contract pays them the same amount as the first contract.
This is in effect a 'bet' that the software will perform effectively. If a bug is discovered, the user is paid a predetermined amount. This amount can be determined by the user to cover the expected costs of patching and any consequential damages (if so desired). This allows the user to select their own risk position by purchasing more or less risk as suits both the risk tolerance and the nature of the user's systems.
Such a derivative (if an open market is allowed to exist) would indicate the consensus opinion as to the security of the software and the reputation of the vendor. Such an instrument would allow software vendors and users to hedge the risks faced by undiscovered software vulnerabilities. These instruments would also be in the interest of the software vendor's investors as the ability to manage risk in advance would allow for forward financial planning and limit the negative impact that vulnerability discovery has on the quoted prices of a vendors capital.
This project will model the security of software coding practices in a manner that will lead to fewer economic externalities

**Utility to Department of Homeland Security**

In economic terms, we want to assign liability such that the optimal damage mitigation strategy occurs. The victim will mitigate their damages where no damages for breach apply in respect of the optimal strategy and payoffs. The rule that creates the best incentives for both parties is the doctrine of avoidable consequences (marginal costs liability).
Mitigation of damages is concerned with both the post-breach behaviors of the victim and the actions of the party to minimize the impact of a breach. In a software parlays', this would incur costs to the user of the software in order to adequately secure their systems. This again is a trade-off. Before the breach (through software failures and vulnerabilities that can lead to a violation of a system's security), the user has an obligation to install and maintain the system in a secure state. The user is likely to have the software products of several vendors installed on a single system. Because of this, the interactions of the software selected and installed by the user span the range of multiple sources and no single software vendor can account for all possible combinations and interactions.
Any pre-breach behavior of the vendor and user of software needs to incorporate the capability of the vendors to both minimize the liability attached to their own products, as well as the interactions of other products installed on a system. It is feasible to deploy one of several options that can aid in the minimization of the effects of a breach due to a software problem prior to the discovery of software vulnerabilities, these include:

1. The software vendor can implement protective controls (such as firewalls)
2. The user can install protective controls
3. the vendor can provide accounting and tracking functions

The following steps further facilitate in minimizing the effects of software vulnerabilities:

1. The vendor can employ more people to test software for vulnerabilities
2. The software vendor can add additional controls

Where more time is expended on the provision of software security by the vendor (hiring more testers, more time writing code etc), the cost of the software needs to reflect this additional effort, hence the cost to the consumer increases. This cost is divisible in the case of a widely deployed Operating System (such as Microsoft Windows) where it is easy to distribute the

incremental costs across additional users. Smaller vendors (such as small tailored vendors for the Hotel accounting market) do not have this distributional margin and the additional controls could result in a substantial increase in the cost of the program.

**Technical Approach**

The goal of this research project is to create a series of quantitative models for information security that can be used to create a software security derivative and insurance market. Mathematical modeling techniques that can be used to model and predict information security risk will be developed using a combination of techniques including:

- Economic theory, and Econometrics
- Quantitative financial modeling,
- Behavioral Economics,
- Algorithmic game theory and
- Statistical hazard/survival models.

The models will account for heteroscedastic confounding variables and include appropriate transforms such that variance heterogeneity is assured in non-normal distributions. Process modeling for integrated Poisson continuous-time process for risk through hazard will be developed using a combination of:

- Business financial data (company accountancy and other records),
- Anti-Virus Industry data
- Legal databases for tortuous and regulatory costs and
- Insurance datasets.

**This work and research follows and continues that published as:**

Wright, Craig S. and Zia, Tanveer A. (2010) T*he Economics of Developing Security Embedded Software*, Proceedings of the 8th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 30th November 2010 Charles Sturt University http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1101&context=ism

and

Wright, Craig S. (2010) *Software, Vendors and Reputation: an analysis of the dilemma in creating secure software*, Proceedings of InTrust 2010 The Second International Conference on Trusted Systems 13th – 15th December 2010 Beijing, P. R. China Charles Sturt University

and (forthcoming)

Wright, Craig S. and Zia, Tanveer A (2011) *A Quantitative Analysis into the Economics of Testing Software Bugs*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011

Wright, Craig S. and Zia, Tanveer A (2011) *A Rationally Opting for the Insecure Alternative: Negative Externalities and the Selection of Security Controls*, CISIS 2011 June 8-10th, 2011

**Personnel and Performer Qualifications and Experience**

**Craig S Wright (Full CV too long and is available in request)**

Over the years Craig has personally conducted and managed in excess of 1,600 IT security related engagements for more than 180 Australian and international organizations in both the private and government sectors. As a strong believer in life-long learning, Craig has qualifications in Law, IT, Mathematics and Business. However, his driving focus is research and development in the security and

risk arena. He is the first person to have obtained multiple GSE certifications (Malware and Compliance) Craig designed the architecture for the world's first online casino (Lasseter's Online) in the Northern Territory; as well he has, in the past, designed and managed the implementation of many of the systems that protect the Australian Stock Exchange. To add to these accomplishments he has authored IT security related books and articles as well as designed a new university program for Charles Sturt University in New South Wales, Australia which will offer a Master in Digital Forensics. This program commenced in 2010 and be offered as an on campus and distance education program.

**Dave Kleiman** (http://en.wikipedia.org/wiki/Dave_Kleiman)

Dave Kleiman is a noted Forensic Computer Investigator, an author/coauthor of multiple books and a noted speaker at security related events

**Bob Radvanovsky**, CIFI, CISM, REM, CIPS, Infracritical, Inc.
Principle, SCADA expert and Author
(chapter author) of "Corporate Hacking and Technology-driven Crime: Social Dynamics and URL:
http://www.amazon.com/Corporate-Hacking-Technology-driven-Crime-Implications/dp/1616928050

URL: http://www.infracritical.com/papers/scadasec-2010-review.zip
URL: http://www.amazon.co.uk/Critical-Infrastructure-Homeland-Emergency-Preparedness/dp/1420095277
URL: http://viewer.zmags.com/publication/d1408139#/d1408139/12
URL: http://www.amazon.com/Transportation-Systems-Security-Allan-McDougall/dp/1420063782

**Commercialization Capabilities and Plan**

The principles are experienced researchers and businessmen in the realm of Information Security. The research will be conducted in conjunction with Charles Sturt University and will follow the standard commercialization processes of the University (these processes are available online). Further, this project will create a large body of public and academic knowledge and scientific research that could also be used by other companies and Universities in the creation of further models and structures that will lead to the securing of more systems again.

**Costs, Work, and Schedule**

| | |
|---|---|
| Amount Requested (in dollars): | $1,200,000.00 |
| Duration: | 36 months |

The funding request will provide full scholarships and positions for three (3) PhD candidates to aide in the research and investigation of software security issues and solution, the creation of economic models and the publication of an expected 20-30 papers in this field. The period is set to three years which includes the completion of the PhD projects and the creation of the market, insurance and derivative models.

- PhD Funding $360,000
- Supervision $180,000
- Survey and data Analysis $220,000
- Administration $120,000
- Core Systems $220,000
- Marketing of system and test use $100,000

| | |
|---|---|
| **BAA Number:** BAA 11-02-TTA 01-0127-WP<br>**Offeror Name:** W&K INFO DEFENSE RESEARCH LLC<br>**Title** Software Derivative Markets & Information Security Risk<br>BAA 11-02-TTA 14-0025-WP<br>**Date:** 07/04/2010 | |
| NA | **Operational Capability:**<br>The project test, develop and test a combination of insurance and derivative based risk markets for both software security and information risk minimization. |
| **Proposed Technical Approach:**<br>This project will address and provide measures and The analysis will measure the following coding errors:<br>• Format string errors<br>• Integer Overflows<br>• Buffer overruns<br>• SQL Injection<br>• Cross-Site scripting<br>• Race Conditions<br>• Command Injection.<br>In addition, market models for selling vulnerabilities will be developed and tested. A first stage vulnerability and risk marketplace will be developed.<br><br>Several published papers have been released (forthcoming include)<br><br>Wright, Craig S. and Zia, Tanveer A (2011) *A Quantitative Analysis into the Economics of Testing Software Bugs*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011<br><br>Wright, Craig S. and Zia, Tanveer A (2011) *A Rationally Opting for the Insecure Alternative: Negative Externalities and the Selection of Security Controls*, Proceedings CISIS 2011 June 8-10th, 2011 | **Schedule, Cost, Deliverables, & Contact Info:**<br>This project will develop the optimal derivative and risk strategy for software markets. A game theoretic approach to this will be modelled looking at the incentives of the business and programming functions in the organization. Programmers, as optimists (Brooks, ) hold,<br>"the first assumption that underlies the scheduling of systems programming is that all will go well".<br>Testing is rarely considered by the normal programmer as this would imply failure. However, the human inability to create perfection leads to the introductions of flaws at each stage of development. This project will deliver frameworks designed to optimize the software development process and to sell the risk using a derivative market place that reflects this risk. The end goal is to remove externalities from the costs of software and incorporate the cost of bad software design into the final cost to the consumer.<br>**Deliverables:**<br>20-30 published papers<br>3 PhD Thesis' in the field<br>A commercial model for software derivatives and insurance markets<br>**Corporate Information:**<br>Dave Kleiman<br>W&K INFO DEFENSE RESEARCH LLC<br>4371 Norhtlake Blvd #314<br>Palm Beach<br>FL 33410 - 6253<br>Phone: 5613108801<br>Email: dave@davekleiman.com |

Authorized Representative: Craig Wright

Signature:

**Proposal White Paper** **(Type II)**

| | |
|---|---|
| **BAA number**, • | BAA 11-02-TTA 05-0155-WP |
| **Title of proposal;** | SCADA Isolation |
| **Name of offeror** | W&K INFO DEFENSE RESEARCH LLC |
| Administrative Contact: | Dave Kleiman |
| Company Name: | W&K INFO DEFENSE RESEARCH LLC |
| Mailing Address (Line 1): | 4371 Norhtlake Blvd #314 |
| Mailing Address (Line 2): | |
| City: | Palm Beach |
| State & Zip Code: | FL 33410 - 6253 |
| Phone: | 5613108801 |
| Fax: | NA |
| TIN: | 274997114 |
| Technical Contact: | Craig Wright |
| Company Name: | W&K INFO DEFENSE RESEARCH LLC |
| Mailing Address (Line 1): | 4371 Norhtlake Blvd #314 |
| Mailing Address (Line 2): | |
| City: | Palm Beach |
| State & Zip Code: | FL 33410 - 6253 |
| Phone: | +61 2 4362 1512 |
| Fax: | NA |
| TIN: | 274997114 |

W&K INFO DEFENSE RESEARCH LLC is a Joint Venture Company between a US Vet. Owned Enterprise and a Australian Research Company.

| | |
|---|---|
| Amount Requested (in dollars): | $1,800,000.00 |
| Duration: | 36 months |
| Requested Starting Date: | 07/04/2011 |
| Business Type: | Small Business |

**Executive Summary**

This project involves the creation of a SCADA targeted filter. This filter will act as a security gateway allowing users to access legacy systems that do not support modern encrypted protocols to do so whist not having to interfere with the existing system. At the same time, advanced threats and Malware (such as STUXNET) will be isolated from the systems using a bridged firewall layer. This system will in itself be isolated and resilient and be capable of reliable action when power and other failures occur. It will collate and report attacks seamlessly allowing Internet connected management and monitoring systems to co-exist on treacherous networks in a cloud environment.

The Revenant device is an embedded Linux-based appliance with an RFC compliant IPSec and Stateful firewall implementation built into the kernel. It is built using embedded Linux and is completely solid state with no moving parts to fail and no hard drive. It also utilises kernel-based IPSec. Designed as an appliance, this system is modular and highly configurable, requiring a small physical, CPU and memory footprint.

The Revenant appliance platform provides a base set of services and functions as an operating environment for many security conscious network based applications. The Appliance provides built-in IPSec encryption, SSHv2 Secure Remote Management, text based management and power-off safe operation.

Basic Management and upkeep of Revenant

System Life-Cycle comprises:

- Security Patch updates
- System and Application updates
- System health-check and maintenance
- System Security Integrity maintenance

Revenant embodies an imbedded, appliance architecture with a strong bias towards encryption, out-of-band authentication and other network applications.

Two primary products have been designed at this point, with expansion into additional modules planned for the future.

- Revenant Encrypted Private Network Gateway
- The Revenant EPN Gateway provides a platform for performing IPSec encryption in several configurations:
  1) Network-to-Network
  2) Host-to-Network
  3) Host-to-Host
  4) Revenant IDS
- The Revenant application is also capable of providing a platform for an IDS sensor.

The Revenant appliance platform provides a base set of services and functions as an operating environment for many security conscious network based applications. The Appliance provides built-in IPSec encryption, SSHv2 Secure Remote Management, Text based management and power-off safe operation

The Revenant appliance has been built with size, performance and security as primary goals, and as a result of this, the system does not run any network accessible processes except those required by specifically installed modules.

The Revenant platform offers no intrinsic network access paths, and is not accessible on the network unless one of the network modules has been installed. The Revenant system does not load any network accessible functionality except as required by the appliance modules loaded in any specific configuration.

The Revenant Measurement appliance is an "Out-of-Band" strong authentication and connection gateway system. Measurement is an access concentrator, which performs strong authentication of user requests. In a security conscious environment, the Measurement allows an organization to effectively provide wide-ranging access to systems or services through a single, secure access path.

The Revenant appliance is a perfect platform for Measurement services due to the security functions and services built into the base system.

### 1.1 Related Work and our contributions

This project involves the creation of a SCADA targeted filter. This filter will act as a security gateway allowing users to access legacy systems that do not support modern encrypted protocols to do so whist not having to interfere with the existing system. At the same time, advanced threats and Malware (such as STUXNET) will be isolated from the systems using a bridged firewall layer. This system will in itself be isolated and resilient and be capable of reliable action when power and other failures occur. It will collate and report attacks seamlessly allowing Internet connected management and monitoring systems to co-exist on treacherous networks in a cloud environment.

**Technical Approach**

A PCap module written in R and C that can take direct network feeds (TCP/IP) and report on anomalous traffic (with a learning feature and feedback cycle to minimize error with use) will be developed with the appliance.

**This work and research follows and continues that published as:**

Wright, Craig S. and Zia, Tanveer A. (2010) T*he Economics of Developing Security Embedded Software*, Proceedings of the 8th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 30th November 2010 Charles Sturt University http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1101&context=ism

and

Wright, Craig S. (2010) *Software, Vendors and Reputation: an analysis of the dilemma in creating secure software*, Proceedings of InTrust 2010 The Second International Conference on Trusted Systems 13th – 15th December 2010 Beijing, P. R. China Charles Sturt University



and (forthcoming)

Wright, Craig S. and Zia, Tanveer A (2011) *A Quantitative Analysis into the Economics of Testing Software Bugs*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011
Wright, Craig S. and Zia, Tanveer A (2011) *A Rationally Opting for the Insecure Alternative: Negative Externalities and the Selection of Security Controls*, CISIS 2011 June 8-10th, 2011

**Personnel and Performer Qualifications and Experience**

**Craig S Wright (Full CV too long and is available in request)**

Over the years Craig has personally conducted and managed in excess of 1,600 IT security related engagements for more than 180 Australian and international organizations in both the private and government sectors. As a strong believer in life-long learning, Craig has qualifications in Law, IT, Mathematics and Business. However, his driving focus is research and development in the security and risk arena. He is the first person to have obtained multiple GSE certifications (Malware and Compliance) Craig designed the architecture for the world's first online casino (Lasseter's Online) in the Northern Territory; as well he has, in the past, designed and managed the implementation of many of the systems that protect the Australian Stock Exchange. To add to these accomplishments he has authored IT security related books and articles as well as designed a new university program for Charles Sturt University in New South Wales, Australia which will offer a Master in Digital Forensics. This program commenced in 2010 and be offered as an on campus and distance education program.

**Dave Kleiman** (http://en.wikipedia.org/wiki/Dave_Kleiman)

Dave Kleiman is a noted Forensic Computer Investigator, an author/coauthor of multiple books and a noted speaker at security related events

**Bob Radvanovsky**, CIFI, CISM, REM, CIPS, Infracritical, Inc.
Principle, SCADA expert and Author
(chapter author) of "Corporate Hacking and Technology-driven Crime: Social Dynamics and URL: http://www.amazon.com/Corporate-Hacking-Technology-driven-Crime-Implications/dp/1616928050

URL: http://www.infracritical.com/papers/scadasec-2010-review.zip
URL: http://www.amazon.co.uk/Critical-Infrastructure-Homeland-Emergency-Preparedness/dp/1420095277
URL: http://viewer.zmags.com/publication/d1408139#/d1408139/12
URL: http://www.amazon.com/Transportation-Systems-Security-Allan-McDougall/dp/1420063782

**Commercialization Capabilities and Plan**

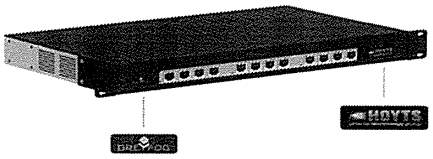
The principles are experienced researchers and businessmen in the realm of Information Security. The research will be conducted in conjunction with Charles Sturt University and will follow the standard commercialization processes of the University (these processes are available online). Further, this project will create a large body of public and academic knowledge and scientific research that could also be used by other companies and Universities in the creation of further models and structures that will lead to the securing of more systems again.

**Costs, Work, and Schedule**

Amount Requested (in dollars): $1,800,000.00
Duration: 36 months

The funding request will provide full scholarships and positions for two (2) PhD candidates to aide in the research and investigation of security issues and solution, the creation of software and IDS tools in this field. The period is set to three years which includes the completion of the PhD projects and the creation of the appliance and related open source software.

- PhD Funding $240,000
- Supervision $180,000
- Survey and data Analysis $120,000
- Administration $120,000
- Core Systems $220,000
- Marketing of system and test use $100,000
- Software coding $340,000
- Electronics and System $480,000

| | |
|---|---|
| **BAA Number:** BAA 11-02-TTA 05-0155-WP<br>**Offeror Name:** W&K INFO DEFENSE RESEARCH LLC<br>**Title** SCADA Isolation<br>**Date:** 07/04/2010 | |
|  | **Operational Capability:**<br>The project test, develop and test a set of software and hardware solutions developed to minimize attacks again SCADA systems. |
| **Proposed Technical Approach:**<br>This project will provide a low cost, high availability and security SCADA security solution through:<br>• System inventory management<br>• Firewall<br>• Anti-virus / anti-malware<br>• Forensic network capture<br>• IP property protection and extrusion reporting<br>• Risk quantification<br>• Advanced traffic filtering and data capture<br>• The idea to be patented – advanced IDS / honeypot | **Schedule, Cost, Deliverables, & Contact Info:**<br>This project involves the creation of a SCADA targeted filter. This filter will act as a security gateway allowing users to access legacy systems that do not support modern encrypted protocols to do so whist not having to interfere with the existing system. At the same time, advanced threats and Malware (such as STUXNET) will be isolated from the systems using a bridged firewall layer. This system will in itself be isolated and resilient and be capable of reliable action when power and other failures occur. It will collate and report attacks seamlessly allowing Internet connected management and monitoring systems to co-exist on treacherous networks in a cloud environment.<br><br>**Deliverables:**<br>5-10 published papers<br>2 PhD Thesis' in the field<br>A commercial appliance<br>A TCPDump filter program<br>**Corporate Information:**<br>Dave Kleiman<br>W&K INFO DEFENSE RESEARCH LLC<br>4371 Norhtlake Blvd #314<br>Palm Beach<br>FL 33410 - 6253<br>Phone: 5613108801<br>Email: dave@davekleiman.com |

Authorized Representative: Craig Wright

Signature:

| | |
|---|---|
| **Proposal White Paper** | **(Type I)** |
| **BAA number**, • | BAA 11-02-TTA 09-0049-WP |
| **Title of proposal;** | Risk Quantification |
| **Name of offeror** | W&K INFO DEFENSE RESEARCH LLC |
| Administrative Contact: | Dave Kleiman |
| Company Name: | W&K INFO DEFENSE RESEARCH LLC |
| Mailing Address (Line 1): | 4371 Norhtlake Blvd #314 |
| Mailing Address (Line 2): | |
| City: | Palm Beach |
| State & Zip Code: | FL 33410 - 6253 |
| Phone: | 5613108801 |
| Fax: | NA |
| TIN: | 274997114 |
| Technical Contact: | Craig Wright |
| Company Name: | W&K INFO DEFENSE RESEARCH LLC |
| Mailing Address (Line 1): | 4371 Norhtlake Blvd #314 |
| Mailing Address (Line 2): | |
| City: | Palm Beach |
| State & Zip Code: | FL 33410 - 6253 |
| Phone: | +61 2 4362 1512 |
| Fax: | NA |
| TIN: | 274997114 |

W&K INFO DEFENSE RESEARCH LLC is a Joint Venture Company between a US Vet. Owned Enterprise and a Australian Research Company.

| | |
|---|---|
| Amount Requested (in dollars): | $2,200,000.00 |
| Duration: | 36 months |
| Requested Starting Date: | 07/04/2011 |
| Business Type: | Small Business |

**Executive Summary**

Using empirical evidence, this research aims to investigate and quantify the root cause of security flaws that act as a source of system compromise. Research into the effects of poor system design, market based risk solutions based on derivative instruments and the impact of common system misconfigurations will be incorporated into multivariate survival models. This research incorporates the economic impact of various decisions as a means of determining the optimal distribution of costs and liability when applied to information security and in particular when assigning costs in computer system security and reliability engineering.

The objective of this research is to produce an innovative modelling architecture designed around information systems security and risk based reliability and survivability analysis. The objectives of the research are:

(1) To address the critical limitations (Jeanblanc & Valchev, 2005) that are associated with reliability engineering in regards to computer systems. This will be completed with competing risks analysis and multivariate survival analysis coupled with a game theoretic approach. Data collected from an analysis of systems in the field will be used to test assumptions. These assumptions (Marti, 2008) include:
    a. constant and homogenous failure rates,
    b. binary failure and univariate reliability,
    c. censoring of failure data, and
    d. independent failures.

(2) To produce a methodology for the creation and testing of hazard and survival models for information systems. This will become a risk based quantitative approach to reliability and survivability engineering.

(3) To incorporate methods that represent the effects of misaligned incentives and their consequence to security controls.

To do this, it is necessary to recognise that information security is a risk function (Anderson, Longley & Kwok, 1994). Paying for too much security can be more damaging in economic terms than not buying enough. This leads to decisions about where the optimal expenditure on damage prevention should lie. This research will investigate who should be responsible for the security failures that are affecting the economy and society and how can this be maximized in order to minimize negative externalities (Cohen, 1976). The conclusions will be presented using an empirical study of software hazard rates and audit failures along with the question of how to enforce liability in a global economy.

The research is intended to address some of the economic issues that are arising due to an inability of assign risk correctly, a failure to measure risk as well as looking at the misalignment of information systems audit and the compliance regime. The externalities that restrict the development of secure software and how the failure of the end user to apply controls makes it less probable that a software vendor will enforce stricter programming controls with failures in the audit and measurement processes are addressed. This includes a look at the misalignment of audit to security. This misalignment is demonstrated to result from the drawing of funds from security in order to provide compliance with little true economic gain (Wright, 2010).

The introduction of Game Theory and Behavioural Economics (Anderson, 2001; Anderson, & Moore, 2006; Varian, 2004) have created a foundation for the rationalisation of information security processes which lead to improved allocation of economic resources. The optimal distribution of economic resources across risk allocations in information system can only lead to

a combination of more secure systems for a lower overall cost. This research will incorporate the game theoretic multi-player decision problem. Agents in the model will be deemed to be rational with well-defined preferences, include the ability to reason strategically using their knowledge and belief of other players and to act according to a combination of both economic "*first thought*" and deep strategic thinking (Nissan, et. al., 2007). Solutions to these models will be sought through a combination of the following game devices:

- Equilibrium: evolutive (steady state) games
- Heterogeneous sequential games
- Rationalisability: deductive reasoning

The models will detail the existence of strictly dominating games where these exist in information security practices and propose methods to improve these models. Existing information security practices in existing organisations will be classified into the following game types:

- Non-cooperative vs. cooperative game
- Strategic vs. extensive game
- Perfect vs. imperfect information

Bounded rationality, behavioural game aspects and other feedback effects will be investigated (Nissan, et. al., 2007). Social capital based on fairness and reciprocity will be defined as it applies to the economically efficient application of risk processes associated with Information systems. Contract Theory will be used to explain the creation of agreements and "*contracts*" in the presence of information asymmetry. This is approached through the combination of adverse selection, moral hazards and the "*signalling game*". In this, adverse selection is defined as the "*Principal not having been informed of the other agent's private information ex-ante*" such as in George Akerlof's "*Market for lemons*" (1970). This application of game theory has been asserted to explain many aspects of the software industries predisposition to create insecure software (Anderson, 2001). Arora, Telang and Xu (2004) asserted that a market-based mechanism for software vulnerabilities would necessarily underperform a CERT-type mechanism. The market that they used was a game theoretic *pricing game*. In the model reported, the players in the market do not report their prices[1]. These players use a model where information is distributed simultaneously to the client of the player and the vendor. The CERT model was touted as being the most favourable solution. The research will demonstrate that the examined "*market*" model is in itself sub-optimal. It both creates incentives to leak information without proper safeguards and creates vulnerability black-markets that rely on waiting until a patch was publically released and only then releasing the patch to the public. This ignores many externalities and assumes the only control is a patch in place of other alternative compensating controls. It is to be demonstrated that there are flaws with this approach that can be solved through the creation of a security and risk derivative market for software. The user would have an upfront estimate of the costs and this could be forced back to the software vendor. Where the derivative costs more than testing, the vendor would conduct more in-depth testing and reduce the levels of bugs (Bacon et. al. 2009).

### 1.2 Our contribution and Technical Approach

We intend to present an analysis using empirical studies to determine and model the cost of finding, testing and fixing security vulnerabilities. The goal of this research project is to create a series of quantitative models for information security. Mathematical modelling techniques that

[1] E.g., iDefense Ltd. and other similar providers have a semi-closed market with limited information exchange.

can be used to model and predict information security risk will be developed using a combination of techniques including:

- Economic theory, and Econometrics
- Quantitative financial modelling,
- Behavioural Economics,
- Algorithmic game theory and
- Statistical hazard/survival models.

The models will account for heteroscedastic confounding variables and include appropriate transforms such that variance heterogeneity is assured in non-normal distributions. Process modelling for integrated Poisson continuous-time process for risk through hazard will be developed using a combination of:

- Business financial data (company accountancy and other records),
- Anti-Virus Industry data
- Legal databases for tortuous and regulatory costs and
- Insurance datasets.

This data will be coupled with hazard models created and validated using Honeynets (e.g. Project Honeynet), reporting sites such as the Internet Storm Centre and iDefence. The combination of this information will provide the framework for a truly quantitative security risk framework[2]. At present, the DShield storm centre receives logging from over 600,000 organisations. This represents a larger quantity of data than is used for actuarial data in the home insurance industry. The problem being that this information is not collated or analysed in any quantitatively sound manner. This research will model survival times for types of applications using the body of research into quantitative code analysis for risk. The research will create a series of models (such as those used within mechanical engineering, material science etc) for Information Risk.

Some of the methods that are planned testing in the creation of the risk framework will include:

- Random forest clustering,
- K-means analysis,
- Other classification algorithms, and
- Network associative maps in text analysis forensic work.

The correlation of reference data (such as IP and functional analysis data) between C&C (Command and Control) systems used in "*botnets*" is one aspect of this research. Starting from the outside (the cloud and perimeter) and working inwards to the network, the risk model would start by assessing external threats and move into internal threat sources, becoming gradually become more and more granular as one moves from network to individual hosts and finally to people (user behaviour (Varian, 2004)) and application modelling (Guo, Jarrow, & Zeng, 2005). The eventual result will be the creation of a model that can incorporate the type of organisation, size, location, application, systems used, and the user awareness levels to create a truly quantitative risk model. This would be reported with SE (standard error) and confidence level rather than a point estimate. Code to import data from hosts and networks, using raw "*pcap traces*"[3] will be developed such that system statistics and other data can be collated into a standardised format. This code will be developed in "R" and "C++". This will enable the

[2] Support has been sought and received from SANS (including DShield), CIS (Centre for Internet Security) and the Honeynet project.
[3] Pcap is a packet capture standard supported by both open source and commercial network capture equipment.

creation and release of actuarial threat risk models that incorporate heterogeneous tendencies in variance across multidimensional determinants while maintaining parsimony. I foresee a combination of Heteroscedastic predictors (GARCH/ARIMA etc) coupled with non-parametric survival models. I expect that this will result in a model where the underlying hazard rate (rather than survival time) is a function of the independent variables (covariates). Cox's Proportional Hazard Model with Time-Dependent Covariates would be a starting point, going to non-parametric methods if necessary. The end goal will be to create a framework and possibly a program that can assess data stream based on a number of dependant variables (Threat models, system survival etc) and covariates and return a quantified risk forecast and standard error.

**Utility to Department of Homeland Security**

When a system fails, it often can fail in numerous ways with several causes for the failure (Crowder 2001). Censored observation management can be considered the principal factor influencing survival analysis. Survival analysis and has developed rigorous procedures and methods effective for the treatment of censored data based on probability theory, asymptotic counting and stochastic process as well as the Martingale central limit theorem. References to the univariate analysis of survival is found in Cox (1972), Cox and Oakes (1984), Fleming and Harrington (1991), Andersen et al (1993), Kalbfleisch and Prentice (1980, 2002), Klein and Moeschberger (2003), Ibrahim et al. (2005), Lawless (1982, 2003), Ma and Krings (2008).

Modeling risk allows it to be measured and controlled.

**<u>This work and research follows and continues:</u>**

Wright, Craig S. and Zia, Tanveer A. (2010) T*he Economics of Developing Security Embedded Software*, Proceedings of the 8th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 30th November 2010

Charles Sturt University

http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1101&context=ism

and (forthcoming)

Wright, Craig S. and Zia, Tanveer A (2011) *A Quantitative Analysis into the Economics of Testing Software Bugs*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011

Wright, Craig S. and Zia, Tanveer A (2011) *A Rationally Opting for the Insecure Alternative: Negative Externalities and the Selection of Security Controls*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011

**Personnel and Performer Qualifications and Experience**

**Craig S Wright (Full CV too long and is available in request)**

Over the years Craig has personally conducted and managed in excess of 1,600 IT security related engagements for more than 180 Australian and international organizations in both the private and government sectors. As a strong believer in life-long learning, Craig has qualifications in Law, IT, Mathematics and Business. However, his driving focus is research and development in the security and risk arena. He is the first person to have obtained multiple GSE certifications (Malware and Compliance) Craig designed the architecture for the world's first online casino (Lasseter's Online) in the Northern Territory; as well he has, in the past, designed and managed the implementation of many of the systems that protect the Australian Stock Exchange. To add to these accomplishments he has authored IT security related books and articles as well as designed a new university program for Charles Sturt University in



New South Wales, Australia which will offer a Master in Digital Forensics. This program commenced in 2010 and be offered as an on campus and distance education program.

**Dave Kleiman** (http://en.wikipedia.org/wiki/Dave_Kleiman)

Dave Kleiman is a noted Forensic Computer Investigator, an author/coauthor of multiple books and a noted speaker at security related events

**Bob Radvanovsky**, CIFI, CISM, REM, CIPS, Infracritical, Inc.

Principle, SCADA expert and Author

URL: http://www.amazon.com/Corporate-Hacking-Technology-driven-Crime-Implications/dp/1616928050

URL: http://www.infracritical.com/papers/scadasec-2010-review.zip

URL: http://www.amazon.co.uk/Critical-Infrastructure-Homeland-Emergency-Preparedness/dp/1420095277

URL: http://viewer.zmags.com/publication/d1408139#/d1408139/12

URL: http://www.amazon.com/Transportation-Systems-Security-Allan-McDougall/dp/1420063782

**Commercialization Capabilities and Plan**

The principles are experienced researchers and businessmen in the realm of Information Security. The research will be conducted in conjunction with Charles Sturt University and will follow the standard commercialization processes of the University (these processes are available online). Further, this project will create a large body of public and academic knowledge and scientific research that could also be used by other companies and Universities in the creation of further models and structures that will lead to the securing of more systems again.

**Costs, Work, and Schedule**

| | |
|---|---|
| Amount Requested (in dollars): | $2,200,000.00 |
| Duration: | 36 months |

The funding request will provide full scholarships and positions for three (3) PhD candidates to aide in the research and investigation of software security issues and solution, the creation of economic models and the publication of an expected 20-30 papers in this field.

The period is set to three years which includes the completion of the PhD projects and the creation of the market, insurance and derivative models.

- PhD Funding $480,000
- Supervision $350,000
- Survey and data Analysis $230,000
- Research Fellowships (2) $260,000
- Administration $120,000
- Costs (Computational Systems) $660,000
- Support Costs (Coding) $300,000

| | |
|---|---|
| **BAA Number:** BAA 11-02-TTA 01-0127-WP<br>**Offeror Name:** W&K INFO DEFENSE RESEARCH LLC<br>**Title** Risk Quantification<br>**Date:** 07/04/2010 | |
| N/A | **Operational Capability:**<br>The research is intended to address some of the economic issues that are arising due to an inability of assign risk correctly, a failure to measure risk as well as looking at the misalignment of information systems audit and the compliance regime. The externalities that restrict the development of secure software and how the failure of the end user to apply controls makes it less probable that a software vendor will enforce stricter programming controls with failures in the audit and measurement processes are addressed. This includes a look at the misalignment of audit to security. This misalignment is demonstrated to result from the drawing of funds from security in order to provide compliance with little true economic gain (Wright, 2010). |

**Proposed Technical Approach:**

The objective of this research is to produce an innovative modeling architecture designed around information systems security and risk based reliability and survivability analysis. The objectives of the research are:

(1) To address the critical limitations (Jeanblanc & Valchev, 2005) that are associated with reliability engineering in regards to computer systems. This will be completed with competing risks analysis and multivariate survival analysis coupled with a game theoretic approach. Data collected from an analysis of systems in the field will be used to test assumptions. These assumptions (Marti, 2008) include:

a. constant and homogenous failure rates,

b. binary failure and univariate reliability,

c. censoring of failure data, and

d. independent failures.

(2) To produce a methodology for the creation and testing of hazard and survival models for information systems. This will become a risk based quantitative approach to reliability and survivability engineering.

(3) To incorporate methods that represent the effects of misaligned incentives and their consequence to security controls.

**Schedule, Cost, Deliverables, & Contact Info:**

**Deliverables:**

30-40 published papers

3 PhD Thesis' in the field

A commercial model for modeling information risk

Several published papers have been released (forthcoming include)

Wright, Craig S. and Zia, Tanveer A (2011) A Quantitative Analysis into the Economics of Testing Software Bugs, Proceedings of CISIS 2011 June 8-10th, 2011

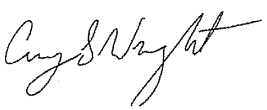
Wright, Craig S. and Zia, Tanveer A (2011) A Rationally Opting for the Insecure Alternative: Negative Externalities and the Selection of Security Controls, Proceedings of CISIS 2011, 2011

**Corporate Information:**

Dave Kleiman
W&K INFO DEFENSE RESEARCH LLC
4371 Norhtlake Blvd #314
Palm Beach
FL 33410 - 6253
Phone: 5613108801
Email: dave@davekleiman.com

Authorized Representative: Craig Wright

Signature:





**Proposal White Paper** **(Type I)**

| | |
|---|---|
| **BAA number**, • | BAA 11-02-TTA 01-0127-WP |
| **Title of proposal;** | Software Assurance through Economic Measures |
| **Name of offeror** | W&K INFO DEFENSE RESEARCH LLC |
| Administrative Contact: | Dave Kleiman |
| Company Name: | W&K INFO DEFENSE RESEARCH LLC |
| Mailing Address (Line 1): | 4371 Norhtlake Blvd #314 |
| Mailing Address (Line 2): | |
| City: | Palm Beach |
| State & Zip Code: | FL 33410 - 6253 |
| Phone: | 5613108801 |
| Fax: | NA |
| TIN: | 274997114 |
| Technical Contact: | Craig Wright |
| Company Name: | W&K INFO DEFENSE RESEARCH LLC |
| Mailing Address (Line 1): | 4371 Norhtlake Blvd #314 |
| Mailing Address (Line 2): | |
| City: | Palm Beach |
| State & Zip Code: | FL 33410 - 6253 |
| Phone: | +61 2 4362 1512 |
| Fax: | NA |
| TIN: | 274997114 |

W&K INFO DEFENSE RESEARCH LLC is a Joint Venture Company between a US Vet. Owned Enterprise and an Australian Research Company.

| | |
|---|---|
| Amount Requested (in dollars): | $650000.00 |
| Duration: | 36 months |
| Requested Starting Date: | 07/04/2011 |
| Business Type: | Small Business |

**Executive Summary**

The deficiency of published quantitative data on software development and systems design has been a major ground for software engineering's failure to ascertain a proper scientific foundation. Past studies into coding practice have focused on software vendors. These developers have many distinctions from in-house projects that are not incorporated into the practices and do not align well with in-house corporate code development. In the past, building software was the only option but as the industry developed, the build vs. buy argument has swung back towards in-house development with the uptake of Internet connected systems. In general, this has been targeted towards specialized web databases and online systems with office systems and mainstream commercial applications becoming a 'buy' decision.

As companies move more and more to using the web and as 'cloud applications' become accepted, in-house development is becoming more common. This paper uses an empirical study of in-house software coding practices in Australian companies to both demonstrate that there is an economic limit to how far testing should proceed as well as noting the deficiencies in the existing approaches.

1.1 Related Work

Other studies of coding processes and reliability have been conducted over the last few decades. The majority of these have been based either on studies of large systems and mainframe based operations or have analyzed software vendors. In the few cases where coding practices within individual organization have been quantitatively analyzed, the organizations have been nearly always large telecommunications firms or have focused on SCADA and other critical system providers.

Whilst these results are extremely valuable, they fail to reflect the state of affairs within the vast majority of organizations. With far more small to medium businesses coupled with comparatively few large organizations with highly focused and dedicated large scale development teams (as can be found in any software vendor), an analysis of in-house practice is critical to both security and the economics of in-house coding.

As the Internet becomes all persuasive, internal coding functions are only likely to become more prevalent and hence more crucial to the security of the organization.

1.2 Our contribution

We intend to present an analysis using empirical studies to determine and model the cost of finding, testing and fixing software bugs. We model the discovery of bugs or vulnerabilities in using quantitative functions and calculate the defect rate per SLOC (source line of codes) using Bayesian calculations.

The end solution to the limited and sub-optimal markets that currently exist would be the creation of Hedge funds for software security. Sales in software security based derivatives could be created on forward contracts. One such solution is the issuing of paired contracts (such as

exist in short sales of stocks ). The first contract would be taken by a user and would pay a fixed amount if the software has suffered from any unmitigated vulnerabilities on the (forward) date specified in the contract. The paired contract would cover the vendor. If the vendor creates software without flaws (or at least mitigates all easily determinable flaws prior to the inception of the contract) the contract pays them the same amount as the first contract.

This is in effect a 'bet' that the software will perform effectively. If a bug is discovered, the user is paid a predetermined amount. This amount can be determined by the user to cover the expected costs of patching and any consequential damages (if so desired). This allows the user to select their own risk position by purchasing more or less risk as suits both the risk tolerance and the nature of the user's systems.

Such a derivative (if an open market is allowed to exist) would indicate the consensus opinion as to the security of the software and the reputation of the vendor. Such an instrument would allow software vendors and users to hedge the risks faced by undiscovered software vulnerabilities. These instruments would also be in the interest of the software vendor's investors as the ability to manage risk in advance would allow for forward financial planning and limit the negative impact that vulnerability discovery has on the quoted prices of a vendors capital.

This project will model the security of software coding practices in a manner that will lead to fewer economic externalities

**Utility to Department of Homeland Security**

The game theoretic approach to this can be modeled looking at the incentives of the business and programming functions in the organization. Programmers are optimists. As Brooks noted, "the first assumption that underlies the scheduling of systems programming is that all will go well". Testing is rarely considered by the normal programmer as this would imply failure. However, the human inability to create perfection leads to the introductions of flaws at each stage of development.

**Technical Approach**

Just as car dealers buff the exterior and detail the upholstery of a used car, neglecting the work that should be done on the engine, software vendors add features. Most users are unlikely to use even a small fraction of these features, yet they buy the product that offers more features over the more secure product with fewer features. The issue here is that users buy the features over security. This is a less expensive option for the vendor to implement and provide.

The creation of a security and risk derivative should change this. The user would have an upfront estimate of the costs and this could be forced back to the software vendor. Where the derivative costs more than testing, the vendor would conduct more in-depth testing and reduce the levels of bugs. This would most likely lead to product differentiation (as occurred in the past with Windows 95/Windows NT). Those businesses who wish to pay for security could receive it. Those wanting features would get what they asked for.

It is argued that software developers characteristically do not correct all the security vulnerabilities and that known ones remain in the product after release. Whether this is due to a lack of resources or other reasons, this is unlikely to be the norm and would be rectified by the market. The cost of vendors in share price and reputational losses exceed the perceived gains from technical reasons where the fix might break existing applications. The application is already broken in the instance of a security vulnerability.

Users could still run older versions of software and have few, if any, bugs. The issue is that they would also gain no new features. It is clear that users want features. They could also choose to use only secure software, but the costs of doing so far outweigh the benefits and do not provide a guarantee against the security of a system being compromised. As such, the enforced legislation of security standards against software vendors is detrimental. A better approach would be to allow an open market based system where vendors can operate in reputational and derivative markets.

At the end of any analysis, security is a risk function and what is most important is not the creation of perfectly security systems, but the correct allocation of scarce resources. Systems need to be created that allow the end user to determine their own acceptable level of risk based on good information.

The goal of this research project is to create a series of quantitative models for information security that can be used to create a software security derivative and insurance market. Mathematical modeling techniques that can be used to model and predict information security risk will be developed using a combination of techniques including:

- Economic theory, and Econometrics
- Quantitative financial modeling,
- Behavioral Economics,
- Algorithmic game theory and
- Statistical hazard/survival models.

The models will account for heteroscedastic confounding variables and include appropriate transforms such that variance heterogeneity is assured in non-normal distributions. Process modeling for integrated Poisson continuous-time process for risk through hazard will be developed using a combination of:

- Business financial data (company accountancy and other records),
- Anti-Virus Industry data
- Legal databases for tortuous and regulatory costs and
- Insurance datasets.

**This work and research follows and continues that published as:**

Wright, Craig S. and Zia, Tanveer A. (2010) T*he Economics of Developing Security Embedded Software*, Proceedings of the 8th Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia, 30th November 2010

Charles Sturt University

http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1101&context=ism

and

Wright, Craig S. (2010) *Software, Vendors and Reputation: an analysis of the dilemma in creating secure software*, Proceedings of InTrust 2010 The Second International Conference on Trusted Systems 13th – 15th December 2010 Beijing, P. R. China

Charles Sturt University

and (forthcoming)

Wright, Craig S. and Zia, Tanveer A (2011) *A Quantitative Analysis into the Economics of Testing Software Bugs*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011

Wright, Craig S. and Zia, Tanveer A (2011) *A Rationally Opting for the Insecure Alternative: Negative Externalities and the Selection of Security Controls*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011

**Personnel and Performer Qualifications and Experience**

**Craig S Wright (Full CV too long and is available in request)**

Over the years Craig has personally conducted and managed in excess of 1,600 IT security related engagements for more than 180 Australian and international organizations in both the private and government sectors. As a strong believer in life-long learning, Craig has qualifications in Law, IT, Mathematics and Business. However, his driving focus is research and development in the security and risk arena. He is the first person to have obtained multiple GSE certifications (Malware and Compliance) Craig designed the architecture for the world's first online casino (Lasseter's Online) in the Northern Territory; as well he has, in the past, designed and managed the implementation of many of the systems that protect the Australian Stock Exchange. To add to these accomplishments he has authored IT security related books and articles as well as designed a new university program for Charles Sturt University in New South Wales, Australia which will offer a Master in Digital Forensics. This program commenced in 2010 and be offered as an on campus and distance education program.

**Dave Kleiman** (http://en.wikipedia.org/wiki/Dave_Kleiman)

Dave Kleiman is a noted Forensic Computer Investigator, an author/coauthor of multiple books and a noted speaker at security related events

**Bob Radvanovsky**, CIFI, CISM, REM, CIPS, Infracritical, Inc.
Principle, SCADA expert and Author
(chapter author) of "Corporate Hacking and Technology-driven Crime: Social Dynamics and Implication", ISBN 1616928050 and 9781616928056, Information Science Publishing, July 2010.

URL: http://www.amazon.com/Corporate-Hacking-Technology-driven-Crime-Implications/dp/1616928050

"Challenges Faced by the SCADASEC Mailing List", Protecting Canada's Critical Infrastructure 2010 Control Systems Security Workshop, sponsored by Royal Canadian Mounted Police (Ontario Technological Crime), Public Safety Canada and Emergency Management Ontario (Critical Infrastructure Assurance Program), Wednesday April 14, 2010 and Thursday, April 15, 2010.
URL: http://www.infracritical.com/papers/scadasec-2010-review.zip
Author of "Critical Infrastructure: Homeland Security and Emergency Preparedness", Second Edition, ISBN 1420095277 and 9781420095272, Taylor & Francis CRC Press, December 2009.
URL: http://www.amazon.co.uk/Critical-Infrastructure-Homeland-Emergency-Preparedness/dp/1420095277
Contributor (introduction speaker) of "The Year in Homeland Security", 2008/2009 Edition (Charles Oldham, editor director), Faircount Media Group.
URL: http://viewer.zmags.com/publication/d1408139#/d1408139/12
Author (co-author) of "Transportation Systems Security", ISBN 1420063782 and 9781420063783, Taylor and Francis CRC Press, May 2008.
URL: http://www.amazon.com/Transportation-Systems-Security-Allan-McDougall/dp/1420063782

**Commercialization Capabilities and Plan**

The principles are experienced researchers and businessmen in the realm of Information Security. The research will be conducted in conjunction with Charles Sturt University and will follow the standard commercialization processes of the University (these processes are available online). Further, this project will create a large body of public and academic knowledge and scientific research that could also be used by other companies and Universities in the creation of further models and structures that will lead to the securing of more systems again.

**Costs, Work, and Schedule**

| | |
|---|---|
| Amount Requested (in dollars): | $650,000.00 |
| Duration: | 36 months |

The funding request will provide full scholarships and positions for three (3) PhD candidates to aide in the research and investigation of software security issues and solution, the creation of economic models and the publication of an expected 20-30 papers in this field.

The period is set to three years which includes the completion of the PhD projects and the creation of the market, insurance and derivative models.

- PhD Funding $240,000
- Supervision $180,000
- Survey and data Analysis $230,000



| | |
|---|---|
| **BAA Number:** BAA 11-02-TTA 01-0127-WP<br>**Offeror Name:** W&K INFO DEFENSE RESEARCH LLC<br>**Title** Software Assurance through Economic Measures<br>**Date:** 07/04/2010 | |
| N/A | **Operational Capability:**<br>The project will analyze a sample of at least 1,000 coding projects using existing static analysis tools, manual code review and related techniques. Where these methods are lacking, proposals and methods to integrate existing methods and to fill the gaps left will be created. |
| **Proposed Technical Approach:**<br>This project will address and provide measures and The analysis will measure the following coding errors:<br>• Format string errors<br>• Integer Overflows<br>• Buffer overruns<br>• SQL Injection<br>• Cross-Site scripting<br>• Race Conditions<br>• Command Injection.<br>Several published papers have been released (forthcoming include)<br><br>Wright, Craig S. and Zia, Tanveer A (2011) *A Quantitative Analysis into the Economics of Testing Software Bugs*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011<br><br>Wright, Craig S. and Zia, Tanveer A (2011) *A Rationally Opting for the Insecure Alternative: Negative Externalities and the Selection of Security Controls*, Proceedings of 4th International Conference on Computational Intelligence in Security for Information Systems CISIS 2011 June 8-10th, 2011 | **Schedule, Cost, Deliverables, & Contact Info:**<br>Provide any milestone decision points that will be required. Describe period of performance and total costs. Include the base performance period cost and length, and estimates of cost and lengths of possible option.<br>**Deliverables:**<br>20-30 published papers<br>3 PhD Thesis' in the field<br>A commercial model for software derivatives and insurance markets<br><br>A means to measure and predict the following coding errors is being developed<br>Format string errors<br>Integer Overflows<br>Buffer overruns<br>SQL Injection<br>Cross-Site scripting<br>Race Conditions<br>Command Injection.<br><br>**Corporate Information:**<br>Dave Kleiman<br>W&K INFO DEFENSE RESEARCH LLC<br>4371 Norhtlake Blvd #314<br>Palm Beach<br>FL 33410 - 6253<br><br>Phone: 5613108801<br>Email: dave@davekleiman.com |

Authorized Representative: Craig Wright

Signature:

# S&T Directorate BAA Cover Sheet A

## Proposal Does Not Contain Proprietary Information

| | |
|---|---|
| Proposal Number: | BAA 11-02-TTA 14-0025-WP |
| Topic: | TTA 14 - Software Assurance MarketPlace (SWAMP) |
| Proposal Title: | Software Derivative Markets & Information Security Risk |
| Company Name: | W&K INFO DEFENSE RESEARCH LLC |
| Mailing Address (Line 1): | 4371 Norhtlake Blvd #314 |
| Mailing Address (Line 2): | |
| City: | Palm Beach |
| State & Zip Code: | FL 33410 - 6253 |
| Phone: | 5613108801 |
| Fax: | |
| TIN: | 274997114 |
| DUNS + 4: | null - |
| CAGE Code: | |
| SIC: | |
| FICE: | |
| Proposal Contains Proprietary Information: | No |
| Amount Requested (*in dollars*): | $1200000.00 |
| Duration: | 36 months |
| Requested Starting Date: | 07/04/2011 |
| Business Type: | Small Business - 50 or Fewer Employees - Annual Gross Revenue - 1 Million or Less<br>Small Business |

This is the annexure marked with the letter M referred to in the Affidavit / ~~Affirmation / Statutory Declaration~~ of Craig S WRIGHT
~~sworn~~/affirmed/~~declared~~ before me at Sydney
on the 4th day of November 2013

~~One page only~~
Page 1 of 4 pages

NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174

# S&T Directorate BAA Cover Sheet A

## Proposal Does Not Contain Proprietary Information

| | |
|---|---|
| Proposal Number: | BAA 11-02-TTA 09-0049-WP |
| Topic: | TTA 09 - Cyber Economics |
| Proposal Title: | Risk Quantification |
| Company Name: | W&K INFO DEFENSE RESEARCH LLC |
| Mailing Address (Line 1): | 4371 Norhtlake Blvd #314 |
| Mailing Address (Line 2): | |
| City: | Palm Beach |
| State & Zip Code: | FL 33410 - 6253 |
| Phone: | 5613108801 |
| Fax: | |
| TIN: | 274997114 |
| DUNS + 4: | null - |
| CAGE Code: | |
| SIC: | |
| FICE: | |
| Proposal Contains Proprietary Information: | No |
| Amount Requested (*in dollars*): | $2200000.00 |
| Duration: | 36 months |
| Requested Starting Date: | 07/04/2011 |
| Business Type: | Small Business<br>Small Business - 50 or Fewer Employees - Annual Gross Revenue - 1 Million or Less |

# S&T Directorate BAA Cover Sheet A

## Proposal Does Not Contain Proprietary Information

| | |
|---|---|
| Proposal Number: | BAA 11-02-TTA 05-0155-WP |
| Topic: | TTA 05 - Secure, Resilient Systems and Networks |
| Proposal Title: | SCADA Isolation |
| Company Name: | W&K INFO DEFENSE RESEARCH LLC |
| Mailing Address (Line 1): | 4371 Norhtlake Blvd #314 |
| Mailing Address (Line 2): | |
| City: | Palm Beach |
| State & Zip Code: | FL 33410 - 6253 |
| Phone: | 5613108801 |
| Fax: | |
| TIN: | 274997114 |
| DUNS + 4: | null - |
| CAGE Code: | |
| SIC: | |
| FICE: | |
| Proposal Contains Proprietary Information: | No |
| Amount Requested (*in dollars*): | $1800000.00 |
| Duration: | 36 months |
| Requested Starting Date: | 07/04/2011 |
| Business Type: | Small Business - 50 or Fewer Employees - Annual Gross Revenue - 1 Million or Less<br>Small Business |

# S&T Directorate BAA Cover Sheet A

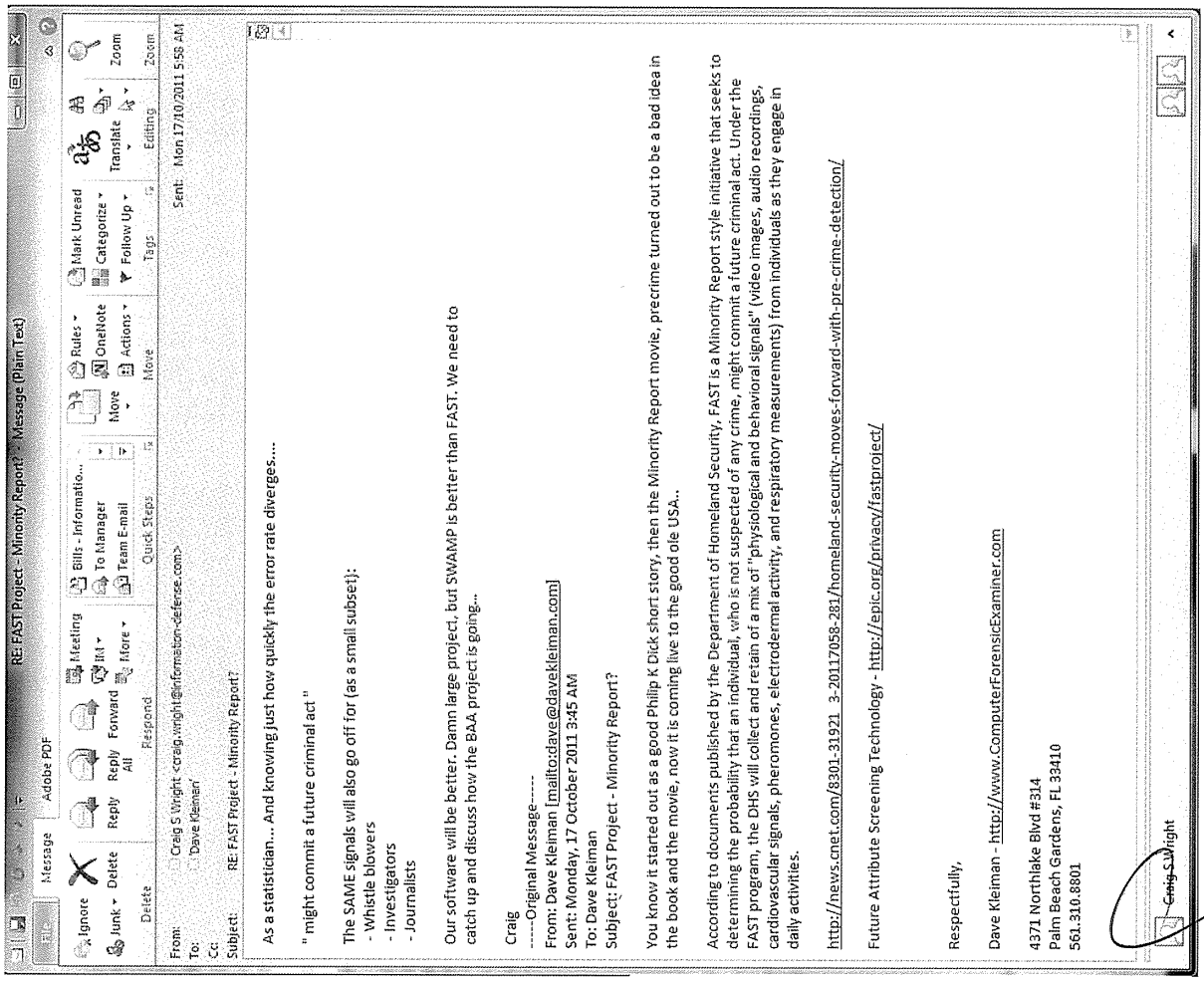
## Proposal Does Not Contain Proprietary Information

| | |
|---|---|
| Proposal Number: | BAA 11-02-TTA 01-0127-WP |
| Topic: | TTA 01 - Software Assurance |
| Proposal Title: | Software Assurance through Economic Measures |
| Company Name: | W&K INFO DEFENSE RESEARCH LLC |
| Mailing Address (Line 1): | 4371 Norhtlake Blvd #314 |
| Mailing Address (Line 2): | |
| City: | Palm Beach |
| State & Zip Code: | FL 33410 - 6253 |
| Phone: | 5613108801 |
| Fax: | |
| TIN: | 274997114 |
| DUNS + 4: | null - |
| CAGE Code: | |
| SIC: | |
| FICE: | |
| Proposal Contains Proprietary Information: | No |
| Amount Requested (*in dollars*): | $650000.00 |
| Duration: | 36 months |
| Requested Starting Date: | 07/04/2011 |
| Business Type: | Small Business<br>Small Business - 50 or Fewer Employees - Annual Gross Revenue - 1 Million or Less |

This is the annexure marked with the letter "L" referred to in the Affidavit / ~~Affirmation / Statutory Declaration~~ of Craig S WRIGHT
~~sworn/affirmed/declered~~ before me at Sydney
on the 4th day of November 2013

~~One page only~~
Page 1 of 1 pages

NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174



RE: FAST Project - Minority Report? - Message (Plain Text)

Message | Adobe PDF

Ignore | Junk | Delete | Reply | Reply All | Forward | Meeting | IM | More | Bills - Informatio... | To Manager | Team E-mail | Move | Rules | OneNote | Actions | Mark Unread | Categorize | Follow Up | Translate | Zoom

Delete | Respond | Quick Steps | Move | Tags | Editing | Zoom

From: Craig S Wright <craig.wright@information-defense.com>
To: 'Dave Kleiman'
Cc:
Subject: RE: FAST Project - Minority Report?
Sent: Mon 17/10/2011 5:58 AM

As a statistician... And knowing just how quickly the error rate diverges....

" might commit a future criminal act "

The SAME signals will also go off for (as a small subset):
- Whistle blowers
- Investigators
- Journalists

Our software will be better. Damn large project, but SWAMP is better than FAST. We need to catch up and discuss how the BAA project is going...

Craig
-----Original Message-----
From: Dave Kleiman [mailto:dave@davekleiman.com]
Sent: Monday, 17 October 2011 3:45 AM
To: Dave Kleiman
Subject: FAST Project - Minority Report?

You know it started out as a good Philip K Dick short story, then the Minority Report movie, precrime turned out to be a bad idea in the book and the movie, now it is coming live to the good ole USA...

According to documents published by the Department of Homeland Security, FAST is a Minority Report style initiative that seeks to determining the probability that an individual, who is not suspected of any crime, might commit a future criminal act. Under the FAST program, the DHS will collect and retain of a mix of "physiological and behavioral signals" (video images, audio recordings, cardiovascular signals, pheromones, electrodermal activity, and respiratory measurements) from individuals as they engage in daily activities.

http://news.cnet.com/8301-31921_3-20117058-281/homeland-security-moves-forward-with-pre-crime-detection/

Future Attribute Screening Technology - http://epic.org/privacy/fastproject/

Respectfully,

Dave Kleiman - http://www.ComputerForensicExaminer.com

4371 Northlake Blvd #314
Palm Beach Gardens, FL 33410
561.310.8801

Craig S Wright

## Integyrs

The following is a response to the request by the ATO, ref. 1011685995901.

## Enterprise

1. Income is on hold at present. The ATO has been auditing and reviewing the company following an initial question as to the allocation of GST that lead to a zero amount in payment overall.
    a. Income was based on an arrangement with a large multi-national form for the export of software and mathematical algorithms.
    b. The company plans to raise money and sell its IP and software.
    c. To do this, it needs to get past the audit phase.
    d. No income is expected to when the ATO allows us to actually carry on a business.
    e. Basically, we are conducting research and developing capital in the hope that one day the auditing process will actually provide some feedback and we can go to market. This was in progress before the ATO started calling clients and placed this on hold.
2. Australia
3. 24x7
4. International
    a. We have published malware papers and processes (peer reviewed)
    b. We have published statistical libraries
    c. These can be sold as .Net framework libraries. Large companies such as Microsoft, MacAfee and CA have interest in the IP, but we need to have cleared the audit before we can sell this.
5. All contract – see 2010 tax return.
    a. Income is on hold to when we can sell
    b. Sales will not start until the audit is complete
    c. Sales had started before the ATO started contacting clients who then placed holds on the sales.
6. All work is currently completed by directors and contractors.

This is the annexure marked with the letter "N" referred to in the Affidavit / Affirmation / Statutory Declaration of Craig S WRIGHT
sworn/affirmed/declared before me at Sydney
on the 4th day of November 2018

One page only
Page 1 of 10 pages

NICHOLAS CHARLES McDONALD
Justice of the Peace Registration 105174

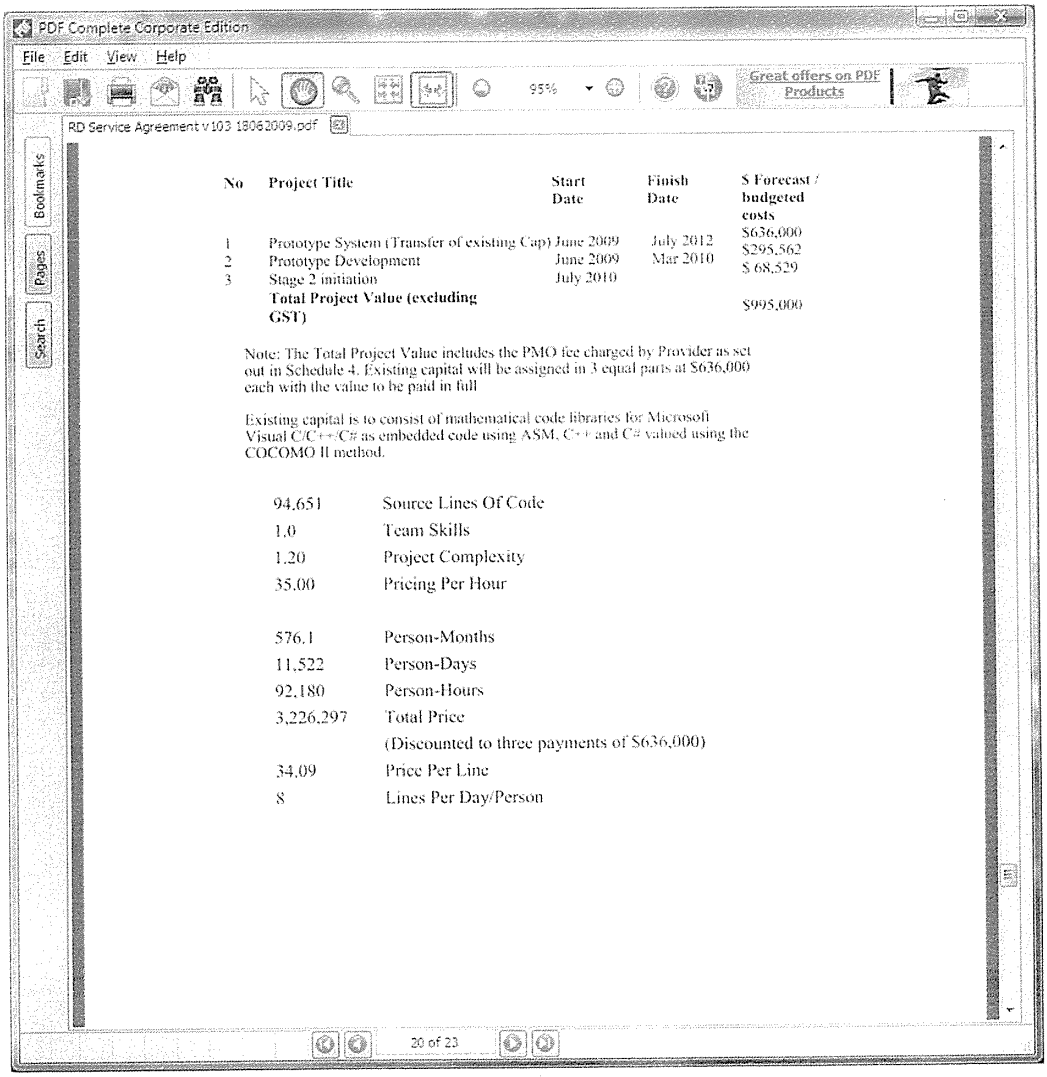
## Supplies

1. Data warehousing
    a. Contracting
    b. Rental of office space
    c. Computer systems
    d. Software
    e. Previously Existing IP
2. See folders.
    a. Q4 2010 has not been completed and hence is not included in this.

## Capital Acquisitions

Plant leasing and core tech.

1. Transfer of developed code into the company.
    a. COCOMO used to cost technology.
2. Leasing of systems for the following 12 months.



PDF Complete Corporate Edition

File Edit View Help

Great offers on PDF Products

RD Service Agreement v103 18062009.pdf

Bookmarks Pages Search

| No | Project Title | Start Date | Finish Date | $ Forecast / budgeted costs |
|---|---|---|---|---|
| 1 | Prototype System (Transfer of existing Cap) | June 2009 | July 2012 | $636,000 |
| 2 | Prototype Development | June 2009 | Mar 2010 | $295,562 |
| 3 | Stage 2 initiation | July 2010 | | $ 68,529 |
| | **Total Project Value (excluding GST)** | | | $995,000 |

Note: The Total Project Value includes the PMO fee charged by Provider as set out in Schedule 4. Existing capital will be assigned in 3 equal parts at $636,000 each with the value to be paid in full

Existing capital is to consist of mathematical code libraries for Microsoft Visual C/C++/C# as embedded code using ASM, C++ and C# valued using the COCOMO II method.

| | |
|---|---|
| 94,651 | Source Lines Of Code |
| 1.0 | Team Skills |
| 1.20 | Project Complexity |
| 35.00 | Pricing Per Hour |
| 576.1 | Person-Months |
| 11,522 | Person-Days |
| 92,180 | Person-Hours |
| 3,226,297 | Total Price |
| | (Discounted to three payments of $636,000) |
| 34.09 | Price Per Line |
| 8 | Lines Per Day/Person |

20 of 23

The IP has been deducted at a rate of 3 years as this is the perceived life of the IP before patient. This is at $666,666 as 1/3rd of the total costs to date.

**Evidence**
See contract – copy on disk

**Capital Value**
Direct costs plus IP

**Valuation**
CoCOMO II based methodology plus direct costs.

**Use in the Enterprise**
The systems and equipment are used directly in the research and the development of solutions that will be offered for international sale.

This Research is directly linked to a PhD candidacy at Charles Sturt University and is related to a CRiCS research study.

The PhD proposal and associated research papers are available on request.

## Other Acquisitions

Non-capital acquisitions for the period 01/01/2010 to 31/21/2010 as per purchase schedule. This includes Carbon credits (to offset computers using electricity) and sundry expenses.

## 2010 Income Tax Return

Invoices – see disk

Payments – see disk

## Loans

– see disk

The following loan contracts have been attached (as prepared by Michie Shehadie and Co and registered).

Loan from Lynn Wright

Loan from Craig Wright

Other Loans (Visa and sundry expenses)

## Current Assets and Liabilities

See MYOB File on disk.

This includes depreciating assets.

These assets are used in the research projects and are key to the development of product.

## Intellectual Property

### Acquisition – how

**R& D intellectual property sold by Craig Wright to Integyrs Pty Ltd**

- You have valued the market value of your intellectual property as $2,246,000 (data from your BAS (Craig Wright) for the tax periods July – Dec 2009) which you sold to two of your companies where you are the Director.
- You have to provide documents to substantiate that you have incurred these costs during the course of your research and development of your intellectual property.
- Please provide substantiation of the above costs by providing the tax invoices with full details of the supplier, date, description and the amounts stated for the purchases.

Sale of Capital Assets to Integyrs Pty Ltd 95 137 033 535

Transfer of code, designs and assets from CSW to Integyrs as of June 30, 2009.

Contracts created by Mitchie Shehadie and Co.

I have attached these documents on the disk and with each sale contract. This includes a schedule as what IP was transferred.

I have attached a spreadsheet with the breakdowns of loans by Lynn Wright for total for a 7% interest rate. The total comes to $815,803.61 as of 01 Jul 2009.

The amounts are covered as follows in the spreadsheet under the following headers:

Conferences and Travel

Lynn paid monies for my attendance at conferences

These where for my business and education (e.g. SANS)

Monthly Contributions

Lynn helped me pay the loans used for the legal costs.

As per the attached information in the attached email, as per 'Farrugia v The Official Receiver (1982) 43 ALR 700' The Doctrine of Exoneration is used in the allocation of these when applied to real property. The loans where for the direct purpose of Integyrs and Research at Lynn's detriment. These amounts are monies she paid towards the loan each month and are hence loaned to the company.

Debt - Purchased contract

DeMorgan Pty Ltd had a contract for $105,000 pa in payments to Lynn on sale.

I purchased this in order to by the business of DeMorgan and start DeMorgan Information Security Systems P/L and this contract and the IP associated with it was transferred into Integyrs.

### Valuation

CoCOMO II for software

Cost basis and transfer for prior assets.

Assets and shares moved from prior companies set as per court order issued by NSW Supreme court.

### Supplier Agreements

Sale of Capital Assets to Integyrs Pty Ltd

Transfer of code, designs and assets from CSW to Integyrs as of June 30, 2009.

$1,100,000

Transfer of code, designs and assets from CSW to Integyrs as of June 30, 2009.

$1,100,000

Associated IP as maintined following – Liquidation of DeMorgan Information Security Systems Pty Ltd and kept due to unpaid debt.

Shares and debt $ 2,178,000

As determined by NSW Supreme Court.

Losses – Depreciation of capital Assets (Write-off)

Old Computer Equipment $22287

Total Gains $2,235,000

Total Losses $34,713

**Bank Statements**

See folder – 1 statement.

AusIndustry

Yes, Integyrs is registered with AusIndustry.

R2010976

# TAB 83-5

# EXHIBIT 5

# CONTRACT FOR THE SALE OF SHARES OF A COMPANY OWNING BUSINESS

**PARTIES**

**Dave Kleiman for W & K Info Defense LLC**
(Vendor)

**AND**

**Craig Wright R&D**
**ABN 97 481 146 384**
(Purchaser)

**AND**

**W&K Info Defense LLC**
(Company)

Ref: CEWK03

**THIS AGREEMENT** dated 02 day of April 2013

**BETWEEN**

Dave Kleiman of W&K Info Defense LLC (Florida)

(Vendor)

And

Craig Wright of Craig Wright R&D
ABN 97 481 146 384

(Purchaser)

And

W&K Info Defense LLC

(Company)

**RECITALS**

**A.** The vendor is the owner of all issued shares in the company being ordinary class shares. Ownership is 50% in the vendor's name and 50% in trust held for the purchaser.

**B.** The company is the owner of and conducts the business known as Bitcoin mining and Software development / Research.

**C.** The vendor has agreed to sell and the purchaser has agreed to purchase the vendor's shares for the price and upon the terms set out hereunder.

**D.** As the purchaser will succeed to the business of the company on completion of the acquisition of these shares, the parties agree that they will incorporate into this agreement those agreements contained in the attached contract for the sale of a business to the intent that they shall in relation to the sale of the shares have the rights and obligations contained in such contract as part of this agreement.

**E.** The company has consented to and agreed to be bound by the terms of this agreement.

**F.** The company includes all software, research material and other aspects of the business.

**G.** The parties wish to commit the terms of their agreement to writing in the manner hereinafter set out.

**OPERATIVE PART**

**1. Interpretation**

This agreement is governed by the laws of the state of NSW, and the parties, submit to the non-exclusive jurisdiction of the courts of that state/country.

In the interpretation of this agreement:

(a) References to legislation or provisions of legislation include changes or re-enactments of the legislation and statutory instruments and regulations issued under, the legislation;

(b) Words denoting the singular include the plural and vice versa; words denoting individuals or persons include bodies corporate and vice versa; references to documents or agreements also mean those documents or agreement as changed, novated or replaced, and words denoting one gender include all genders;

(c) Grammatical forms of defined words or phrases have corresponding meanings;

(d) Parties must perform their obligations on the dates and times fixed by reference to the capital city of the state of Sydney;

(e) Reference to an amount of money is a reference to the amount in the lawful currency of the Commonwealth of Australia;

(f) If the day on or by which anything is to be done is a Saturday, a Sunday or a public holiday in the place in which it is to be done, then it must be done on the next business day;

(g) References to a party are intended to bind their executors, administrators and permitted transferees; and

(h) Obligations under this agreement affecting more than one party bind them jointly and each of them severally.

**2.** The vendor hereby agrees to sell and the purchaser hereby agrees to purchase ordinary class shares in the company for the purchase price as noted below:

(a) Two (2) loans issued under deed "CEWK01" are agreed to be repaid in full for the consideration of 300,000 Bitcoin agreed in the contract. The repayments as a one off of both loans for $20,000,000 with a total value of

$40,000,000 are deemed paid in full for the above value. This is noted as consideration from the purchaser and is issued in forbearance of the requirements of the contract signed 22 April 2011 between the Vendor/Company and the purchaser (designated CEWK01).

(b) The vendor agrees that the paper wallet with address "1933phfhK3ZgFQNLGSDXvqCn32k2buXY8a" held in escrow will be released to the purchaser.

(c) Due to the unexpected rise in the value of Bitcoin, it is agreed that two transfers (in Bitcoin) of BTC 125,000 and BTC 125,500 when taken in conjunction with the supply of the software, will suffice to fulfil the contract.

**3.** Hence, the vendor will:

(a) Pay (transfer to) the purchaser 250,500 BTC on 30 April 2013,

(b) Accept transfer of the escrowed Bitcoin paper wallet to the purchaser,

(c) Transfer the ASC hardware to the purchaser,

(d) Release the source code to the purchaser,

(e) Transfer the Vistomail email account.

(f) Transfer all research materials from the four (4) DHS BAA research projects to the purchaser with all notes, data and results, and

(g) Transfer any shares in the company to the purchaser by 30 April 2013.

**4.** The Purchaser will:

(a) Accept the new terms in full satisfaction of the contract with Reference CEWK01 made between the vendor/company and the purchaser on 22 April 2013.

(b) Accept the vendor's 323,000 remaining "mined" Bitcoin as a 49.5% stake in a new venture to be formed in Australia (to be called Coin-Exch Pty Ltd) between the vendor and the purchaser for the exploitation of the joint and to be pooled Bitcoin

(c) Accept the transfer of the 323,000 Bitcoin (to be made on the 30th April 2013) as capital and note that shares in the new enterprise will be issued at this point.

(d) Provide $30,000,000 in capital into Coin-Exch Pty Ltd (to be formed) and the software developed in the prior venture.

**5.** Settlement shall be effected on 30 April 2013.

**6.** So far as they are relevant the agreements contained in the incorporated contract for the sale of a business shall be agreements between the parties herein.

**7.** In the event of either party failing to complete this agreement on the settlement date then the other shall be entitled at any time thereafter to serve a notice to complete requiring the other to complete within 14 days from the date of service of the notice, which time period is considered reasonable by both parties. For the purpose of this contract, such notice to complete shall be deemed both at law and in equity sufficient to make time of the essence of this contract.

**8.** On the settlement date the vendors shall:

(a) Deliver up to the purchaser possession of the business conducted by the company and in all respects shall have complied with the terms of the business sale contract incorporated herein;

(b) Deliver up to the purchaser duly executed instruments of transfer of their shares;

(c) Cause a meeting of the directors of the company to be held at which the directors shall approve and consent to the sale and transfer by the vendors to the purchaser of the vendors' shares.

(d) Send all software developed under the various DHS BAA filings to the purchaser (incl. source code and documentation).

(e) Provide the location and access rights to the ASC mining hardware hosted at a site known to Mr Kleiman will be returned with this transfer. This has a nominal value of $8,828,571.29 before depreciation. This is a

(f) Solutions to the Agent and Merkle Tree problems developed by Professor David Reese.

(g) Bitcoin agent software and suit of C/C++/C# and Python Blockchain software source codes.

(h) Exchange Bitcoin holdings as noted in the contract.

**9.** The company hereby agrees to take all steps and carry out all acts to procure the registration on the settlement date of the purchaser as the registered holder of tile to the vendors' shares.

**10.** The purchaser will make all reasonable endeavours to have the new venture (Coin-Exch Pty Ltd) registered for GST and under the Australian Corporations act provisions before settlement on the 30th April 2013.

**11.** The parties hereto agree to execute and perform all such acts, deeds, documents and things whatsoever as may be necessary and desirable to better carry into effect the provisions of this agreement.

**12. Vendor's warranties**

(a) **Vendor's authority to sell**

(i) The vendors are the registered and beneficial owners of their shares in the company.

(ii) The vendors have full power and authority to sell and transfer to the purchaser good legal and equitable title to the shares without the consent or authorisation of any person except only consents required by the company.

(b) **The company's financial statements**

Other than matters disclosed to the purchaser in writing the books and accounts of the company truly and fairly reflect the company's affairs.

(c) **Books and records**

The company's books, records and registers are in the possession of the company, and accurately record the details of all of the company's transactions, finances, assets and liabilities.

(d) **Taxation**

(i) Other than disclosed to the purchaser in writing the company has lodged or filed all tax and duty returns for all taxes including GST, income tax, sales tax, fringe benefits tax, payroll tax, group tax and WorkCare levies.

(ii) No claim has or will be made against the company for payment by the company pursuant to the provisions of the Income Tax Assessment Act 1936 of any tax which is not shown or included as a liability or provision in the balance sheet contained in the accounts.

(iii) Neither the commissioner nor any federal, state or municipal body has any dispute with the company concerning the company's affair.

(e) **Compliance with applicable laws**

(i) Neither the vendor nor the company has breached, or caused a breach of the company's memorandum or articles of association; any contract, agreement or instrument which binds the company; or any judgment, order, injunction or decree of any court, commission or administrative body relating to the company or to the shares.

(ii) Neither the company nor any of its officers, agents or employees (while performing their duties for the company) has breached the law. The company has not been notified that it has, or may have, breached the law regulating its affairs or the conduct of its business.

(f) **Litigation and indebtedness**

Other than as disclosed to the purchaser in writing:

(i) The company is not a party to, or threatened with, any claim, litigation, prosecution or arbitration in any court, tribunal or otherwise;

(ii) There are no unsatisfied judgments or arbitral awards against the company;

(iii) The company is not being investigated for any breach of the law. Neither the company nor any of its directors is aware of any breach of the law or of any circumstances, which would give rise to a breach of the law other than as disclosed to the purchaser in writing;

(iv) The company has met all deadlines for repayment of its debts;

(v) No petitions, notices or proceedings have come to the company's notice, which could result in it being wound up. No orders or resolutions have been made or passed to place the company in liquidation or provisional liquidation.

(g) **Accuracy of disclosed information**

(i) The vendor has disclosed to the purchaser all information, which would be material for a purchaser in forming a decision whether or not to purchase the shares.

(ii) If either the vendor or the company becomes aware of anything which may constitute a breach of, or be inconsistent with any representation, warranty or undertaking in this agreement, they will notify the purchaser of its particulars promptly in writing.

(h) **Warranties and indemnities**

(i) It is a condition of this agreement that each warranty is true and correct in every respect and shall be construed separately.

(ii) The vendor acknowledges that the warranties have been given with the intention and for the purpose of inducing the purchaser to enter into this agreement.

(iii) The purchaser has entered into this agreement and agreed to the purchase price payable for the shares on the basis of and in full reliance upon the warranties.

(iv) Prior to the settlement date the vendor will take all such steps and provide all such information and documents with regard to the company as the purchaser may reasonably require and will give the purchaser and its professional advisers full and free access to the records and accounts of the company (whether financial or otherwise) to enable them to fully investigate the accuracy of the warranties.

**13. Notices**

A communication required by this agreement, by a party to another, must be in writing and may be given to them by being:

(a) Delivered personally; or

(b) Posted to their address specified in this agreement, or as later notified by them, in which case it will be treated as having been received on the second business day after posting; or

(c) Faxed to the facsimile number of the party with acknowledgment of receipt received electronically by the sender, when it will be treated as received on the day of sending; or

(d) Sent by email to their email address, when it will be treated as received on that day.

**14. Waiver or variation**

(a) A party's failure or delay to exercise a power or right does not operate as a waiver of that power or right.

(b) The exercise of a power or right does not preclude:

(i) Its future exercise; or

(ii) The exercise of any other power or right.

(c) The variation or waiver of a provision of this agreement or a party's consent to a departure from a provision by another party will be ineffective unless in writing executed by the parties.

**15. Counterparts**

This agreement may be executed in any number of counterparts each of which will be an original but such counterparts together will constitute one and the same instrument and the date of the agreement will be the date on which it is executed by the last party.

**16. Further assurance**

Each party will from time to time do all things (including executing all documents) necessary or desirable to give full effect to this agreement.

**17. Costs**

Each party will pay their own costs in relation to this agreement.

**SIGNED AS AN AGREEMENT**

Executed by
W & K Info Defense LLC )

Dave Kleiman

Dave Kleiman
DIRECTOR

Executed by
Craig Wright R&D (A.B.N. 97 481 146 384)

Craig S Wright